DISRUPTING HARM IN MALAYSIA

Evidence on online child sexual exploitation and abuse

Funded by End Violence Against Children

Implemented by ECPAT INTERPOL unicef Office of Research-Innocenti

Warning:
Disrupting Harm addresses the complex and sensitive topic of online child sexual exploitation and abuse. At times in the report, some distressing details are recounted, including using the direct words of survivors themselves. Some readers, especially those with lived experiences of sexual violence, may find parts of the report difficult to read. You are encouraged to monitor your responses and engage with the report in ways that are comfortable. Please seek psychological support for acute distress.

Suggested citation:
ECPAT, INTERPOL and UNICEF. (2022). *Disrupting Harm in Malaysia: Evidence on online child sexual exploitation and abuse*. Global Partnership to End Violence Against Children.

Funding from the Global Partnership to End Violence Against Children, through its Safe Online initiative, does not constitute endorsement.

CONTENTS

MESSAGE FROM THE MINISTRY OF WOMEN, FAMILY AND COMMUNITY DEVELOPMENT AND THE MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

The Ministry of Women, Family and Community Development (KPWKM) and the Ministry of Communications and Multimedia Malaysia (K-KOMM) welcome the completion of the *Disrupting Harm in Malaysia* study, and would like to congratulate ECPAT, INTERPOL, and UNICEF on their efforts to complete this research.

In a highly connected society like Malaysia, having a strong evidence base around children's internet use, and the harms they might encounter online, is of the utmost important. While children have a lot to gain from being online, there are also serious harms that they might be exposed to including online sexual exploitation and abuse (OCSEA). It is for this reason that KPWKM together with K-KOMM through Malaysian Communications and Multimedia Commission (MCMC) have championed and supported the *Disrupting Harm* project. The *Disrupting Harm* in Malaysia report provides an in-depth look at the nature and scope of online child sexual exploitation and abuse (OCSEA) in Malaysia, as well as assessing the capacity of our national response systems to tackle these forms of sexual violence against children.

Malaysia has already taken concrete steps to address these crimes against children including the adoption of the ASEAN Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in 2019, which is part of our commitment to further strengthen our child protection standards and policies on OCSEA.

Crimes against children that are committed online or that are facilitated via digital technologies introduce a new set of challenges that our policy makers, judiciary, law enforcement, frontline responders and wider communities must grapple with. With the rapid changes of technology, so too does the pattern of offending change, and this requires our response systems to be agile, adaptable, and informed by evidence. This report ends with a set of recommendations which have been workshopped during a national consultation in April 2022. These recommended ways forward call on all relevant stakeholders to act together to collectively improve our ability to protect children from harm. Ending these forms of violence against children is a shared responsibility and it is therefore the Ministries' hope that all relevant sectors can work collaboratively to turn evidence into action.

The Ministry of Women, Family and Community Development and the Ministry of Communications and Multimedia Malaysia once again congratulate ECPAT International, INTERPOL and UNICEF Office of Research – Innocenti, and the Global Partnership to End Violence Against Children on completing this project and looks forward to further accelerating our efforts to tackle these crimes against children and keeping them safe online.

YBhg. Dato' Sri Haji Mohammad Bin Mentek
Secretary General,
Ministry of Communication and Multimedia Malaysia

YBhg. Datuk Dr. Maziah binti Che Yusoff
Secretary General,
Ministry of Women, Family and Community Development

MESSAGE FROM THE END VIOLENCE PARTNERSHIP

Our online lives are constantly advancing. The internet and rapidly evolving digital communication tools are bringing people everywhere closer together. Children are increasingly conversant with and dependent on these technologies, and the COVID-19 pandemic has accelerated the shift online of many aspects of children's lives.

The internet is a powerful tool for children to connect, explore, learn and engage in creative and empowering ways. The importance of the digital environment to children's lives and rights was emphasised by the United Nations' Committee on the Rights of the Child in General Comment No. 25 adopted in 2021. The General Comment also stresses the fact that spending time online inevitably brings unacceptable risks and threats of harm, some of which children also encounter in other settings and some of which are unique to the online context.

One of the risks is the misuse of the internet and digital technologies for the purpose of child sexual exploitation and abuse. Online grooming, sharing of child sexual abuse material and live-streaming of child abuse are crimes against children that need an urgent, multi-sectoral and global response. These crimes are usually recorded in the form of digital images or videos, which are very often distributed and perpetually reshared online, victimising children over and over again. As risks of harm continue to evolve and grow exponentially, prevention and protection have become more difficult for governments, public officials and providers of public services to children, but also for parents and caregivers trying to keep up with their children's use of technology.

With progress being made towards universal internet connectivity worldwide, it is ever more pressing to invest in children's safety and protection online. Governments around the world are increasingly acknowledging the threat of online child sexual exploitation and abuse, and some countries have taken steps to introduce the necessary legislation and put preventive measures in place. At the same time, the pressure is mounting on the technology industry to put the safety of children at the heart of design and development processes, rather than treating it as an afterthought. Such safety by design must be informed by evidence on the occurrence of online child sexual exploitation and abuse. *Disrupting Harm* makes a significant contribution to that evidence.

The Global Partnership to End Violence against Children, through its Safe Online initiative, invested US$7 million in the *Disrupting Harm* project. *Disrupting Harm* uses a holistic and innovative methodology and approach to conduct a comprehensive assessment of the context, threats and children's perspectives on online child sexual exploitation and abuse. This unprecedented project draws on the research expertise of ECPAT, INTERPOL and UNICEF Office of Research – Innocenti, and their networks. The three global partners were supported by ECPAT member organisations, the INTERPOL National Central Bureaus and the UNICEF Country and Regional Offices. It is intended that the developed and tested methodology be applied in other countries around the world.

FOREWORD

Disrupting Harm represents the most comprehensive and large-scale research project ever undertaken on online child sexual exploitation and abuse at the national level and has resulted in 13 country reports and a series of unique 'data insights'. It provides comprehensive evidence concerning the risks children face online, how they develop, how they interlink with other forms of violence and what can be done to prevent them.

This research in Malaysia would not be possible without support from the Government of Malaysia. Our gratitude is extended to the Malaysian Communications and Multimedia Commission (MCMC) for their leadership in chairing the Disrupting Harm National Taskforce in Malaysia, chaired by Mr Zulkarnain Mohd Yasin and vice-chair Ms Eneng Faridah Iskandar, to facilitate in-country research and to Ministry of Women, Family, and Community Development (MWFCD) for their leadership and role in overall child welfare and protection work.

The findings will serve governments, industry, policy makers, and communities to take the right measures to ensure the internet is safe for children. This includes informing national prevention and response strategies, expanding the reach of *Disrupting Harm* to other countries and regions, and building new data and knowledge partnerships around it.

Disrupting harm to children is everyone's responsibility.

Dr Howard Taylor
Executive Director
End Violence Partnership

EXECUTIVE SUMMARY

Funded by the Global Partnership to End Violence against Children, through its Safe Online initiative, ECPAT International, INTERPOL and UNICEF Office of Research – Innocenti worked in partnership to design and implement *Disrupting Harm* – a research project on online child sexual exploitation and abuse (OCSEA). This unique partnership brings a multidisciplinary approach to a complex issue in order to present multiple viewpoints around the issue of OCSEA. The research was conducted in seven Eastern and Southern African countries and six Southeast Asian countries, including Malaysia. Data are synthesised from up to nine different research activities to generate each national report which tells the story of the threat of OCSEA and the national response mechanisms in place to tackle this form of violence against children. The report ends with a set of clear recommendations for action.

Internet access, activities and skills

Ninety-four percent of 12–17-year-olds in Malaysia are internet users, meaning that they have used the internet within the past three months. Moreover, according to the *Disrupting Harm* nationally representative household survey of 995 internet-using children in this age group, 96% go online at least once a day. Children mainly access the internet from their homes, followed by access at school and at malls/internet cafes. Almost all the children surveyed used smartphones to access the internet, and only 25% – particularly the younger children aged 12–13 – shared their smartphones with someone else. Computers were used for internet access by 28% of children.

The majority of the surveyed children used social media (91%) and instant messaging apps (90%), watched video clips (88%) and used the internet for schoolwork (86%) at least once a week. Children in Malaysia are high-frequency internet users, and this is reflected in their digital skills. As many as 84% claimed that they could determine which images of themselves or their friends to share online, while 67% said they knew how to change their privacy settings and 66% said that they knew how to report harmful content on social media. Self-reported digital skills were weakest among younger children aged 12–13 and children living in rural areas.

One caregiver[1] of each child interviewed also took part in the survey. Almost all of the surveyed caregivers (98%) said that they had used the internet within the past three months: an unusual finding in the *Disrupting Harm* countries where children were frequently found to be online more than their caregivers. Of the internet-using caregivers, 92% went online every day; however, fewer older caregivers (aged 50+) used the internet as compared to younger caregivers.

As many as 88% of the children surveyed said that their caregivers had suggested ways for them to stay safe online and 79% said that their caregivers would help them if they were bothered by something on the internet. In contrast, caregivers themselves were only moderately confident about their digital skills, i.e., 55% said that they knew more about the internet than their child and 33% said that they could help their child cope with things that bothered them online 'a fair amount'.

Risky online activities

The great majority of the surveyed caregivers considered it to be very risky for children to share sexual images or videos online (87%), send someone their personal information (84%), see sexual images online (83%) or meet someone in person whom they had first encountered online (77%). Twenty-six percent of the children said that their caregivers restricted their use of the internet, while 36% of the caregivers said that they would restrict their children's internet use if the children were bothered by something online.

1. In the household survey, the term 'caregiver' is an inclusive term used to refer to all adults who are responsible for children, such as parents, step-parents, grand-parents or other legal guardians.

Most of the children were also aware of the risks associated with being online. Indeed, only a small minority of children reported that they had engaged in risky online activities in the past year. For example, 5% had, within the past year, met someone in person whom they had first met online. Only 1% (six children) said that they had shared naked pictures or videos of themselves online in the past year.

Twenty-four percent of children had unexpectedly come across sexual content online through advertisements, social media feeds, search engines and messaging apps, and 17% reported actively looking for such material. Children aged 16–17 and boys were the most likely groups to be exposed to sexual images and videos online.

Children's experiences of online sexual exploitation and abuse

The surveyed children were also asked whether they had been subjected to a range of experiences which could constitute OCSEA within the past year. In the *Disrupting Harm* reports, OCSEA is defined as situations that involve the use of digital or communication technologies at some point during the continuum of sexual exploitation or abuse of a child. According to *Disrupting Harm* data, in the past year, 4% of internet-using children aged 12–17 in Malaysia (38 children) reported that they had been subjected to a clear form of online sexual exploitation and abuse. This estimate includes having been blackmailed to engage in sexual activities, having had their sexual images shared without permission, or having been coerced to engage in sexual activities through promises of money or gifts. In addition, 5% of the surveyed children (46 children) had received unwanted requests to talk about sex and 3% (26 children) had received requests for images showing their private parts, which, depending on the circumstances, could constitute grooming. With respect to the household survey, a certain degree of under-reporting is expected due to factors including discomfort about discussing sex and sexuality with survey administrators and fears of legal self-incrimination, as some practices are criminalised.

According to Disrupting Harm data, in the past year, 4% of internet-using children aged 12–17 in Malaysia (38 children) reported that they had been subjected to a clear form of online sexual exploitation and abuse.

Of the 38 children who reported being subjected to at least one of the four clear forms of OCSEA, the offenders were individuals the children did not know prior to the incident (10 children), peers under 18 (six children), adult friends or acquaintances (five children) or family members (five children). Eighteen children did not know who the offender was, while another 11 children preferred not to indicate who the offender was. Children who had been subjected to online sexual exploitation and abuse or experienced other unwanted online interactions of a sexual nature cited numerous social media and online messaging sites where they were targeted. Among these, WhatsApp was most prominent, alongside Facebook/Facebook Messenger. Other non-U.S.-based platforms, particularly WeChat and Telegram, were cited in some instances.

Furthermore, the number of reports (known as CyberTips) made to the U.S. National Center for Missing and Exploited Children (NCMEC) by U.S.-based technology companies concerning suspected child sexual exploitation in Malaysia increased by 90% between 2017 and 2019. A wide range of social media platforms, image hosting and video sharing providers made reports regarding content concerning Malaysia, but the largest number came from Facebook. Almost all notifications were related to the possession, manufacture and distribution of child sexual abuse materials (CSAM). Further analyses for *Disrupting Harm* indicated that there is evidence that, in Malaysia, CSAM is searched for on the open web. Data was identified and shared with Malaysian law enforcement regarding attempted online enticement of children pre-travel, indicating that Malaysia is a potential destination for travelling sex offenders.

Disclosure and reporting of online sexual exploitation and abuse

The law enforcement entity charged with investigating all forms of online and offline child sexual exploitation and abuse is the D11 division of the Royal Malaysia Police (also known as the Sexual, Women and Child Investigation Division). According to the D11 division, 35 cases of OCSEA were investigated between 2017 and 2019. This is the sub-section of all the child abuse cases investigated by the unit that were tagged as involving technology. The D11 division also noted that some of their cases may not have been recorded as OCSEA but may still have had an online or technological element.

OCSEA cases were generally reported to the police by or with the support of adults, i.e., not directly by the children themselves. Only one case came via a helpline. The results from the household survey of children suggest that OCSEA frequently goes undisclosed and formally unreported. Half of the small number of children who did, during the survey, disclose that they were subjected to at least one of the four clear instances of OCSEA or other unwanted sexual experiences on the internet did not tell anyone (indicating possible under-reporting, as mentioned above, meaning that the actual number is likely higher). Those who did disclose were most likely to confide in a friend or a caregiver. Reasons given by children for not disclosing OCSEA included a lack of awareness of where to report or whom to tell, feelings of shame and embarrassment, not thinking the incident serious enough to report, a sense of having done something wrong, concerns about getting into trouble, concern that disclosing would cause trouble for the family, concern that the incident would not be kept confidential, and not believing that anything would be done about it. Conversations with young survivors of OCSEA conducted for *Disrupting Harm* indicated that threats are also used against children. Children – particularly boys – who were abused or exploited by offenders of the same sex may have particular difficulty in disclosing OCSEA due to stigma and the risk of self-incrimination, as sexual contact between males is illegal in the country and a male child could, therefore, be prosecuted under these laws if victimised by a male offender.

Identification and investigation of OCSEA cases

The Sexual Offences against Children Act criminalises the act of sexually communicating with a child or encouraging a child to sexually communicate by any means. It also makes it an offence for anyone to communicate with a child with the intention of committing or facilitating offences related to CSAM or sexual abuse. The act contains a broad definition of CSAM and outlaws many acts related to its production, distribution and sale. Knowingly accessing and possessing CSAM is also an offence. Although respondents in interviews for *Disrupting Harm* reported that these provisions are used in cases of live-streaming of child sexual abuse, the law could more explicitly criminalise this crime. Inconsistencies exist, for example, under the Penal Code, statutory rape – denoted as penetrative sexual intercourse – is only applied to girls below the age of 16. The age of consent for non-penetrative sexual acts, which fall under the Penal Code's "acts of gross indecency", is set at 14 for all children, while the provisions of the Sexual Offences against Children Act apply to all children below the age of 18. In practice, such inconsistencies may lead to different levels of protection depending on the sex and age of the children involved in the abuse.

In the case studies collected from law enforcement for *Disrupting Harm*, male offenders who committed OCSEA-related crimes against male victims were charged under provisions outlawing homosexuality included in the Penal Code as opposed to specific OCSEA-related crimes under the Sexual Offences against Children Act. A lack of familiarity with this act may, in part, explain this tendency, yet this may affect the services and support made available to child victims.

The Malaysia Internet Crime Against Children (MICAC) Investigation Unit is one of the units that make up the D11 division. It comprises four trained officers dedicated to addressing OCSEA at the national headquarters. Despite its expertise, equipment, and strong history of international cooperation and collaboration with financial institutions, the unit is constrained by the low number of staff, frequent transfers and reassignments of duties and responsibilities, the absence of a high-speed broadband connection that would facilitate the use of INTERPOL's International Child Sexual Exploitation database, the lack of psychological support for officers and an insufficient capacity for covert investigations, open-source intelligence gathering and proactive surveillance.

Digital forensic assistance is available to D11/MICAC from the Malaysian Communications and Multimedia Commission (MCMC) and the National Cybersecurity Agency. Under the Malaysia Cyber Security Strategy for 2020–2024, a National CyberCrime Enforcement Plan is to be adopted, which will include efforts to increase the knowledge and skills of law enforcement officers and members of the judiciary and legal professions in the increasingly complex realm of cybercrime.

Children's experiences with law enforcement mechanisms, the justice process and social services

The *Disrupting Harm* research team was unable to identify a sample of children who had sought justice for OCSEA through the courts. Sample identification included extensive searches via the networks of supporting organisations, legal professionals and others. The conclusions drawn in the report, therefore, are based solely on interviews with government officials, justice professionals and a survey of frontline service providers. The difficulty of identifying children may indicate that OCSEA remains insufficiently visible within the justice system on a national level. The possible reasons for this, including evidence that indicates that significant stigma exists around disclosing sexual crimes in Malaysia, is discussed in the report.

Law enforcement officials all expressed their commitment to a child-centred approach to investigations and prosecutions. The D11 division provides support services for children through care officers at Victim Care Centres and liaises with the Department of Social Welfare to obtain other necessary support services for children who have disclosed child sexual exploitation and abuse, including OCSEA (e.g., shelter). There are Child Interview Centres in every state with officers trained to follow child-friendly investigation approaches. Even so, it was reported that the police do not always use the centres' special rooms or video recording equipment when interviewing children.

Two special courts were established to specifically handle sexual crimes against children, in the cities of Putrajaya and Kuching, but this initiative has not yet been expanded to other geographical locations. Special courts have child-friendly facilities, such as private entrances and exits for child victims, child-friendly waiting rooms and video link facilities. Judges use child-friendly language and cases proceed relatively rapidly. In other courts, cases can be drawn out and the treatment of child victims varies, depending on the budgets for facilities or the awareness/training of judicial professionals.

Legal companion services are available to victims through the Legal Aid Department, but interviewees indicated that they are not well defined and are rarely taken up. Similarly, victims have the right to compensation, but prosecutors rarely put in applications, and there is no formal guidance for the courts regarding how to determine the amounts awarded. In addition, offenders may be unable to pay compensation and can choose to serve longer prison terms instead, meaning the child may not benefit from the compensation claims even if pursued.

Social support services for child victims are provided by the Social Welfare Department and various other institutions and organisations. Hospital-based One-Stop Crisis Centres and the Suspected Child Abuse and Neglect teams provide an initial medical examination and non-emergency interventions for sexual crimes, including when children are involved, and they are said to be very efficient in this regard. However, there is a need for clear referral pathways from local clinics to these centres. Social support services are said to be available mostly in major cities.

Current initiatives for children

Malaysia has produced a number of strategic documents on child protection, including a multi-sectoral Plan of Action on Child Online Protection (2015–2020). In 2019, Malaysia adopted the ASEAN Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse. This requires it to improve child protection standards and policies on OCSEA, thus enhancing the capabilities of professionals in the specialised unit responsible for investigating OCSEA-related crimes, strengthening data collection mechanisms, raising awareness and engaging with the private sector.

The main institutions with a mandate for combating OCSEA include the Ministry of Women, Family and Community Development, the Social Welfare Department of Malaysia, the Malaysian Communications and Multimedia Commission (MCMC), Cybersecurity Malaysia, the Ministry of Science, Technology and Innovation, the Royal Malaysia police, the Attorney Generals Chambers, the Ministry of Health and the Ministry of Education. These institutions have carried out awareness-raising and educational initiatives for both children and caregivers concerning child abuse and online safety; however, it was not clear from the interviews with government representatives how much focus is given to OCSEA in these programmes. The MCMC also assists the Royal Malaysia Police by blocking access to websites containing child sexual abuse materials and helping with suspect identification and digital forensic analyses.

However, government representatives and other informants suggested that a lack of dedicated budgets and trained personnel has made it difficult to concretely implement policies and plans to prevent and respond to OCSEA. With respect to coordination, a Child Online Protection Taskforce was established by the Ministry of Women, Family and Community Development in 2013 for the purpose of overseeing the Plan of Action on Child Online Protection – which lapsed in 2020 – but is no longer functioning. Evidence regarding the effectiveness of awareness-raising initiatives related to OCSEA was also not uncovered.

Awareness-raising efforts have been stunted by cultural discomfort around discussing sex and sexuality, which extends into discomfort around sexual abuse and exploitation. This was evidenced in interviews among justice professionals and in the survey with frontline workers, 72% of whom believed taboos around sex and sexuality are a barrier to reporting OCSEA.

Non-governmental organisations (NGOs) cooperate with the government on education and awareness-raising initiatives. NGOs such as Protect and Save the Children, the Women's Aid Organisation and the Women's Centre for Change, Penang, also support victims during court proceedings. Protect and Save the Children is said to be the only social organisation focused solely on child sexual abuse, with a range of activities from policy advocacy to running a hotline and counselling and therapy services. Monsters Among Us: Youth Advocates is a youth-led organisation that aims to advocate, empower, educate and support child victims of abuse. It has an online reporting portal for victims called Lapor Predator.

Internet service providers are said to cooperate well with law enforcement authorities in the investigation of cases of OCSEA. However, this is not obligatory, and in the absence of any mandatory data retention/preservation law, they may not retain and preserve data with this in mind. Similarly, there is no specific legal obligation for Internet service providers to report CSAM or to remove or block access to websites containing child sexual abuse materials; however, the Communications and Multimedia Act makes them criminally liable if they provide content on their networks that is indecent, obscene or offensive in character with the intent to annoy, abuse, threaten or harass. According to the Malaysian Communications and Multimedia Content Code, "child pornography" is included within the category of prohibited obscene content.

Key insights

The report concludes by providing six key insights from the research:

1. In the past year, at least 4% of internet-using children aged 12–17 in Malaysia were subjected to clear instances of online sexual exploitation and abuse, including being blackmailed to engage in sexual activities, having their sexual images shared without permission, or being coerced to engage in sexual activities through promises of money or gifts. Scaled to the population, this represents an estimated 100,000 children who may have been subjected to any of these harms in the span of a single year.
2. According to the household survey, while offenders of OCSEA are often someone unknown to the child, in some cases offenders are individuals the child already knows – often an adult acquaintance, a peer under 18 or a family member.
3. Children mainly experienced OCSEA through the major social media providers, most commonly via WhatsApp, Facebook/Facebook Messenger, WeChat or Telegram.
4. Children who were subjected to OCSEA tended to confide in people within their interpersonal networks, particularly friends, caregivers or siblings. Helplines and the police were almost never utilised to seek help.
5. A range of promising initiatives driven by government, civil society and industry are underway in Malaysia; however, weak interagency coordination and cooperation and limitations related to budgetary resources exist.
6. Although existing legislation, policies and standards in Malaysia include provisions relevant to OCSEA, including strong provisions regarding child-friendly investigations and prosecutions, support to implement such standards across the country and further legislative reform are needed for a comprehensive response to OCSEA.

> **Children who were subjected to OCSEA tended to confide in people within their interpersonal networks, particularly friends, caregivers or siblings. Helplines and the police were almost never utilised to seek help.**

The report ends with a series of detailed recommendations regarding action to be taken by the government, by the law enforcement, justice and social services sectors and by those working within them, by communities, teachers and caregivers, and by digital platforms and service providers. Many of the recommendations align with the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN.[2] These are too detailed to be recounted in the Executive Summary but can be found on page 100 of this report.

2. ASEAN Secretariat. (2021). Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN: Supplement to the ASEAN Regional Plan of Action on the Elimination of Violence Against Children.

DISRUPTING HARM METHODS

As with all the settings in which children live and grow, the online environment can expose them to risks of sexual exploitation and abuse. However, the scarcity of the available evidence makes it difficult to grasp the nature of the harm caused or to make constructive recommendations concerning public policies for prevention and response. Informed by the 2018 WeProtect Global Alliance Threat Assessment,[3] the Global Partnership Fund to End Violence Against Children, through its Safe Online initiative, decided to invest in research to strengthen the evidence base on OCSEA, with a particular focus on 13 countries across Eastern and Southern Africa and Southeast Asia.

The countries of focus in the Southeast Asian region are Cambodia, Indonesia, Malaysia, the Philippines, Thailand and Vietnam. The countries of focus in the Eastern and Southern Africa region are Ethiopia, Kenya, Mozambique, Namibia, South Africa, Tanzania and Uganda.

ECPAT, INTERPOL and UNICEF Office of Research – Innocenti worked in collaboration to design and implement the *Disrupting Harm* project. In total, the three organisations collected data for nine unique research activities. Extensive data collection took place in Malaysia from early 2020 through until November 2021. This was followed by intensive triangulation, which resulted in a series of 13 country reports. The data analysis for Malaysia was finalised in April 2022. Using the same methodology in all participating countries also allows for inter-country comparisons. In addition, the findings and suggested steps are expected to be relevant to a broader global audience.

The desired outcome of this report is to provide a baseline and evidence for policy makers in Malaysia to tackle and prevent online child sexual exploitation and abuse (OCSEA) and strengthen support to children. The recommended actions in the report are aligned with the Model National Response[4] and contribute to the 2030 Agenda for Sustainable Development.[5]

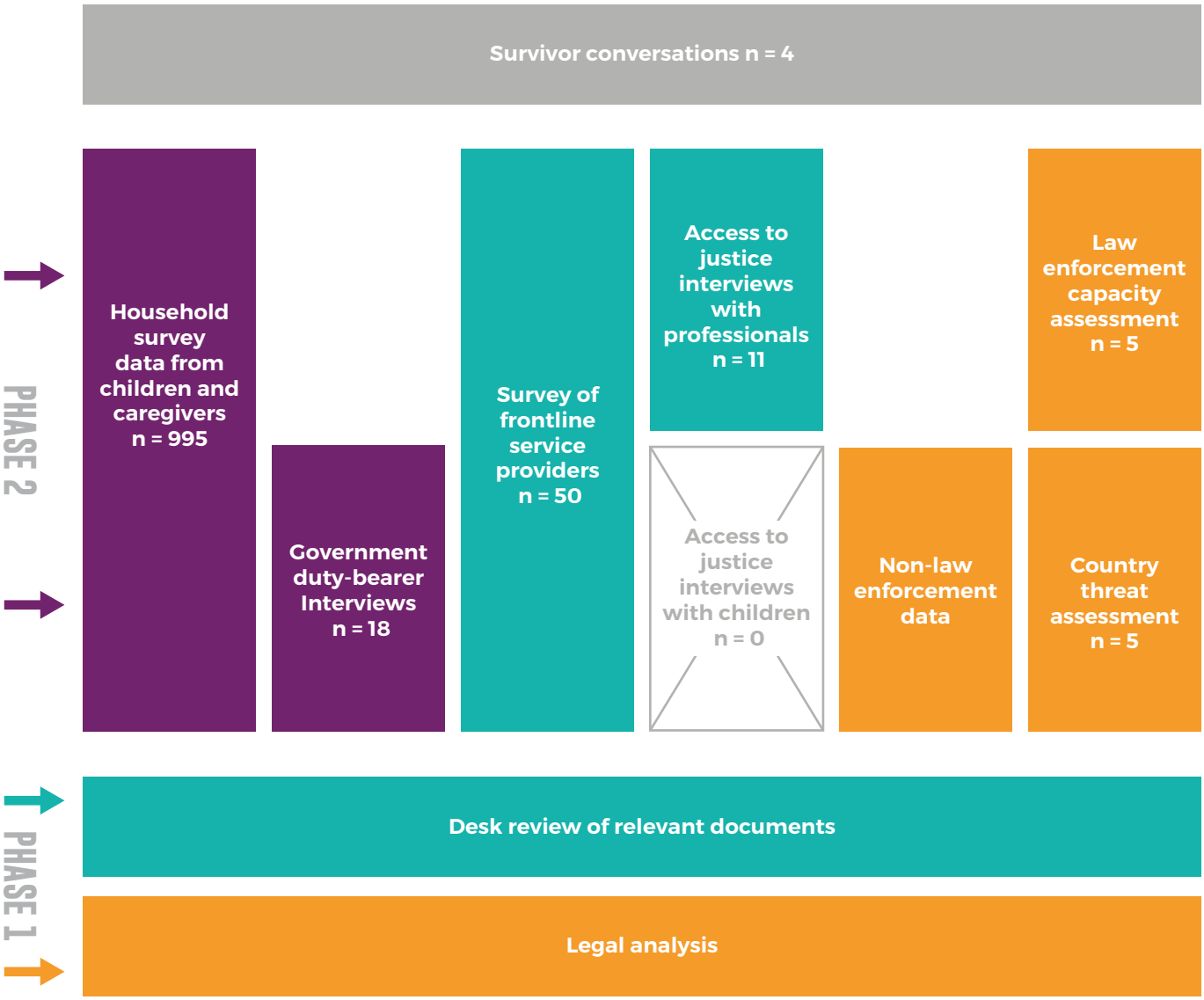
Summary of methods used by ECPAT International in Malaysia

Government duty-bearer[6] interviews

Between July and September 2020, 11 semi-structured interviews were conducted with a total of 18 senior national government representatives[7] whose mandates include OCSEA. As a result of the COVID-19 pandemic, some interviews were conducted in person and others virtually. More information concerning the methodology can be found here, while the preliminary report of this data can be found here. Attributions to data from these respondents have ID numbers beginning with RA1 throughout the report.[8]

3. WeProtect Global Alliance (2018). Global Threat Assessment 2018: Working together to end the sexual exploitation of children online. London: WeProtect Global Alliance.
4. WeProtect Global Alliance (2016). Preventing and Tackling Child Sexual Exploitation and Abuse: A model national response. London: WeProtect Global Alliance.
5. United Nations. (n.d.) Sustainable Development Goals. See: Goals 5.2, 8.7 and 16.2.
6. In this instance, duty-bearers are defined as those who hold specific responsibilities for responding to the risks of OCSEA at a national level.
7. The senior national duty-bearers were from the following government departments and ministries: the Attorney General 's Chambers; the Malaysian Communications and Multimedia Commission; the Ministry of Women, Family and Community Development; the Legal Affairs Division, Prime Minister's Department; the Ministry of Health; the Human Rights Commission; the Department of Social Welfare; the Ministry of Education; Cybersecurity Malaysia; the National Population and Family Development Board, and Royal Malaysia Police.
8. The format RA1-MY-01-A is used for IDs. 'RA1' indicates the research activity, 'MY' denotes Malaysia, '01' is the participant number and 'A' indicates the participant when interviews included more than one person.

Figure 1: *Disrupting Harm* methods in Malaysia.



Analysis of non-law enforcement data and consultations

A range of non-law enforcement entities can provide data and insight on the nature and scale of OCSEA. Data was obtained from the International Association of Internet Hotlines (INHOPE),[9] the Internet Watch Foundation[10] and Child Helpline International.[11] Qualitative insight was provided by a number of global technology platforms. Where relevant, this information supplements the analysis contributed by INTERPOL (see below).

Frontline social service providers' survey

A non-probability convenience sample of 50 client-facing frontline workers in Malaysia (obtained by reaching out to a set of NGOs), including outreach youth workers, social workers, case managers, psychologists and health and legal professionals working directly with children's cases, participated in a survey administered online from August to November 2020. This research activity aimed to explore the scope and context of OCSEA as it is observed by those working on the social support front line. More information on the methodology can be found here, while the preliminary summary report of this data can be found here. Attributions to data from these respondents have ID numbers beginning with RA3 throughout the report.

Access to justice interviews with OCSEA victims[12] and their caregivers

This activity was not undertaken in Malaysia. The research team approached 32 civil society organisations working on Child Rights and Child Protection in an effort to identify victims of OCSEA whose cases had been through the criminal justice system. The majority of the organisations contacted reported that they had not handled any cases of OCSEA. At least two organisations indicated that they had handled OCSEA cases but did not wish to disclose or share the details of the OCSEA victims.

A small number of organisations also confirmed that they had handled OCSEA cases, but the victims had declined to be interviewed. Although the Royal Malaysia Police confirmed they had some OCSEA cases on their register, tracing the victims for the purpose of participating in the *Disrupting Harm* research was a challenge. Additionally, the prosecution for children offences unit in the Attorney General's office and the registrar and judge of the special court for children had no records of cases of OCSEA that had been prosecuted. The Director of Public Prosecutions and the Department of Social Welfare did not have records of OCSEA cases reported and prosecuted either. The perspectives of OCSEA victims and their caregivers are, therefore, unfortunately not represented in the Malaysia report. More information concerning the methods used in this research activity (conducted in countries in which a sample was identified) can be found here.

Access to justice interviews with justice professionals

Ten semi-structured interviews were conducted with eleven criminal justice professionals between July and September 2020. The sample included who had experience with OCSEA criminal cases.[13] More information on the methodology can be found here, while the preliminary summary report of the data can be found here. Attributions to data from these respondents have ID numbers beginning with RA4 throughout the report. The suffix 'justice' is also included in the ID numbers to indicate the interviews with justice professionals.

Literature review and legal analysis

A literature review was undertaken to inform the research teams prior to primary data collection. A comprehensive analysis of the legislation, policy and systems addressing OCSEA in Malaysia was conducted and finalised in June 2020. More information concerning the methodology can be found here, while the full report on the legal analysis can be found here.

9. A global network of 46 member hotlines. INHOPE supports the network in combating child sexual abuse material. For more information see: https://www.inhope.org/EN.
10. UK-based organisation working to remove online child sexual abuse content hosted anywhere in the world. For more information see: https://www.iwf.org.uk/.
11. Child Helpline International collects knowledge and data from child helpline members, partners and external sources. For more information see: https://www.childhelplineinternational.org/about/.
12. The term 'OCSEA victims' refers to their role as victim in the criminal justice process.
13. The following state and non-state agencies were represented in the interviews: the Court of Children in Kuala Lumpur; Voices of the Children; the Attorney General's Chamber; Women's Aid Organisation; Protect and Save the Children; the Legal Aid Department; Royal Malaysia Police and Special Court for Sexual Crimes Against Children.

Conversations with OCSEA survivors[14]

Unstructured one-on-one conversations led by trauma-informed expert practitioners were arranged with 33 young survivors of OCSEA in five of the *Disrupting Harm* countries (nine girls in Kenya, five boys and seven girls in Cambodia, seven girls in Namibia, four girls in Malaysia and one boy in South Africa). The participants were aged between 16 and 24 but had all been subjected to OCSEA as children. Although they were not possible in all countries, these conversations are meant to underline common themes and issues in all 13 *Disrupting Harm* countries. For this reason, the survivor conversations were analysed collectively for all countries. The Malaysia report presents data from the four survivor conversations in Malaysia.

More information concerning the methodology can be found here. The report presenting the analysis of all 33 survivor conversations will be released separately in 2022. Attributions to data from these respondents have ID numbers beginning with RA5 throughout the report.

Summary of methods used in Malaysia by INTERPOL

Quantitative case data analysis

Data was sought on cases related to OCSEA from law enforcement authorities via the INTERPOL National Central Bureau in each country. Data was also obtained from the mandated reports of U.S.-based technology companies to the National Center for Missing and Exploited Children (NCMEC) and from a number of other partner organisations with a view to deepening the understanding of relevant offences committed in the country, offender and victim behaviour, crime enablers and vulnerabilities. Crime data was analysed for the three years from 2017 to 2019.

Qualitative capacity assessments

In addition to seeking data on OCSEA cases, INTERPOL requested data on the capacity of the national law enforcement authorities to respond to this type of crime and interviewed serving officers. Particular emphasis was placed on human resources, access to specialist equipment and training, investigative procedures, the use of tools for international cooperation, achievements and challenges. Attributions to data from this activity have ID numbers beginning with RA8 throughout the report. More information concerning INTERPOL's methodologies can be found here.

Summary of methods used in Malaysia by UNICEF Office of Research – Innocenti

Household survey of internet-using children and their caregivers

In order to understand children's use of the internet, the risks and opportunities they face online and their specific experiences of OCSEA, a nationally representative household survey was conducted face-to-face with 995 internet-using children while adhering to the COVID-19-related restrictions and procedures in force in the country at the time. The term 'household survey' is used throughout the report to indicate findings that come from this specific research activity. The target population for the survey was children aged 12–17 in Malaysia who had used the internet in the three months prior to the interview. The survey sample was composed of 517 (52%) boys and 478 (48%) girls. Of these children, 306 (31%) were 12–13-year-olds, 336 (34%) 14–15-year-olds and 353 (35%) 16–17-year-olds.

In order to achieve a nationally representative sample, the survey was conducted using random probability sampling with national coverage. Coverage is defined as the proportion of the total population that had a chance of being included in the survey sample – meaning that the fieldwork would cover the area where they live if sampled. In Malaysia, the fieldwork coverage was 94% and included the Borneo states. Rural areas that are very remote or isolated were excluded.

14. The term OCSEA survivor refers to children who were victimised but may no longer identify with the term victim as they are on the path of healing.

The sampling followed a three-stage random probability clustered sample design. In the first stage, 100 primary sampling units were selected. The primary sampling units' list was provided by the Department of Statistics Malaysia. In the second stage, interviewers selected addresses in the field using random walk procedures and attempted contact at the selected addresses to screen for members of the survey population using a screening question developed for this purpose. In the third stage, individuals (children and caregivers) were selected within each eligible household using random methods.

In every household visited, an attempt was made to collect data on the number of 12–17-year-old children in the household, their gender and whether they had used the internet in the three months prior. This allowed the researchers to estimate internet penetration rates for all 12–17-year-old children in Malaysia.

The fieldwork took place between April 2021 and November 2021. Data collection was coordinated by Ipsos MORI and carried out by Ipsos Malaysia on behalf of UNICEF Office of Research – Innocenti.

In order to enhance the precision of the estimates, the household survey data used throughout this report was weighted following best practice approaches for the weighting of random probability samples. The weighting included the following stages:

- Designing weight adjustments to reflect the probabilities of selection (inverse probability weights);
- Non-response weights to reduce non-response bias;
- Post-stratification weights to adjust for differences between the sample and population distributions.

A more detailed explanation of the methodological approach and the specific methods used for the analysis of the household survey data can be found here.

Ethical approval

UNICEF Office of Research – Innocenti and ECPAT both received ethical clearance for their research components from the Medical Research and Ethics Committee. The protocols of both ECPAT and UNICEF were also reviewed and approved by the Health Media Lab Institutional Review Board.

INTERPOL assessed both the threat of OCSEA and the capacity of law enforcement to counter this threat. Both assessments involved interviews with law enforcement officers in relevant units in the crime area, and relevant police units and national agencies that manage police data. INTERPOL did not have any contact with the children or victims. Nevertheless, to ensure proper ethical conduct and research standards, the INTERPOL team completed an online course on Responsible Conduct of Research from the Collaborative Institutional Training Initiative. Furthermore, all research activities were implemented in accordance with INTERPOL's Code of Conduct.

National consultation

In a national consultation that took place on 25 April 2022, representatives from government, law enforcement, civil society and other sectors were asked to provide input on the *Disrupting Harm* findings and recommended actions to enhance their relevance for the national context.

ABOUT ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

***Child sexual abuse* refers to various sexual activities perpetrated against children (persons under 18), regardless of whether or not the children are aware that what is happening to them is neither normal nor acceptable. It can be committed by adults or peers and usually involves an individual or group taking advantage of an imbalance of power. It can be committed without explicit force, with offenders frequently using authority, power, manipulation or deception.[15]**

Child sexual exploitation involves the same abusive actions. However, an additional element of a threat or exchange for something (e.g., money, shelter, material goods, immaterial things such as protection, a relationship), or even the mere promise of such, must also be present.[16]

> ***Online child sexual exploitation and abuse* (OCSEA)** refers to situations involving *digital, internet* and *communication technologies* at some point during the continuum of abuse or exploitation. OCSEA can occur fully online or through a mix of online and in-person interactions between offenders and children.

Disrupting Harm focuses on how technology can be misused to facilitate child sexual exploitation and abuse. Its use of the term OCSEA does not refer to abuse or exploitation that occurs exclusively online, nor is it the intention of *Disrupting Harm* to create an artificial divide between online and offline child sexual exploitation and abuse. Children can be abused or exploited while they spend time in the digital environment, but equally, offenders can use digital technology to facilitate their actions, e.g., to document and share images of in-person abuse and exploitation or to groom children to meet them in person.

Disrupting Harm also focuses on how technology facilitates child sexual exploitation and abuse and contributes the evidence needed to understand the role that digital technology plays in sexual violence against children.

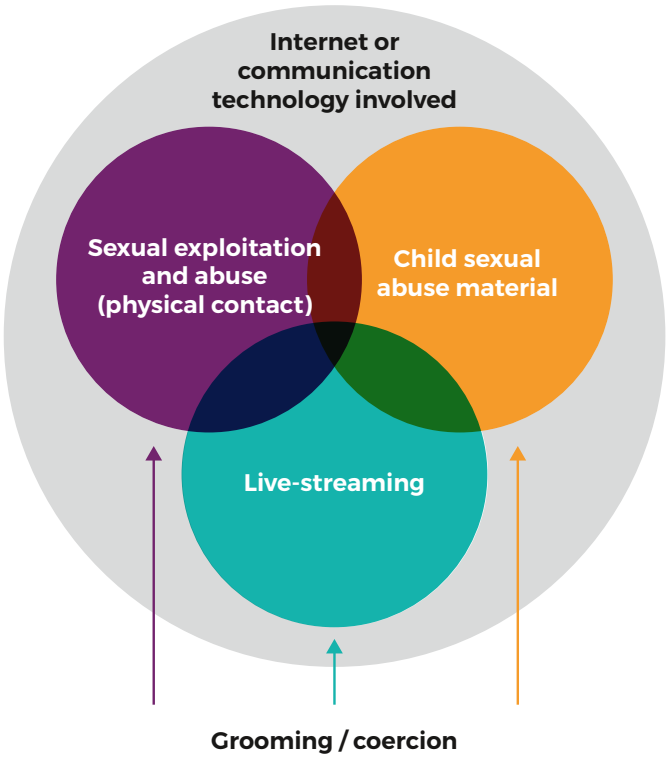
Any characterisation of OCSEA must recognise that the boundaries between online and offline behaviour and actions are increasingly blurred[17] and that responses need to consider the whole spectrum of activities in which digital technologies may play a part. This characterisation is particularly important to keep in mind as children increasingly see their online and offline worlds as entwined and simultaneous.[18]

For *Disrupting Harm*, OCSEA was defined specifically to include child sexual exploitation and abuse that involves the following:

- Production, possession, or sharing of **child sexual abuse material (CSAM):** Photos, videos, audios or other recordings, or any other representation of real or digitally generated child sexual abuse or the sexual parts of a child for primarily sexual purposes.[19]
- **Live-streaming of child sexual abuse:** Child sexual abuse that is perpetrated and viewed simultaneously in real time via communication tools, video conferencing tools and/or chat applications. In most cases, the offender requesting the abuse in exchange for payment or other material benefits is physically in a different location from the child(ren) and the facilitators of the abuse.
- **Online grooming of children for sexual purposes:** Engagement with a child via technology with the intent of sexually abusing or exploiting the child.

15. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 18.
16. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 18, 24.
17. May-Chahal, C., & Palmer, C. (2018). Rapid Evidence Assessment: Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation. Independent Inquiry into Child Sexual Abuse. UK: Lancaster University.
18. Stoilova, M., Livingstone, S., Khazbak, R. (2021). Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes. *Innocenti Discussion Papers* no. 2021-01, Florence: UNICEF Office of Research – Innocenti.
19. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 40.

Figure 2: Framing the main forms of online child sexual exploitation and abuse explored by *Disrupting Harm*.



While international legal instruments[20] criminalising grooming indicate that this must take place with intent to meet the child in person, it has become increasingly common for offenders to sexually abuse children by, for example, manipulating them into self-generating and sharing CSAM through digital technologies, without necessarily having the intention of meeting them and abusing them in person.

The *Disrupting Harm* reports also address other phenomena that contribute to understanding the contexts and socio-cultural environments in which OCSEA occurs.

- **The sharing of self-generated sexual content involving children**[21] can lead to or be part of OCSEA, even if this content is initially produced and shared voluntarily between peers, as it can be passed on without permission or obtained through deception or coercion.
- **Sexual extortion of children**[22] refers to the use of blackmail or threats to extract sexual content or other benefits (e.g., money) from the child, often using sexual content of the child that has previously been obtained as leverage.
- **Sexual harassment of a child**[23] and **unwanted exposure of a child to sexual content**[24] are other phenomena which can constitute or enable OCSEA in some instances. For example, offenders can deliberately expose children to sexual content as part of grooming to desensitise them to sexual acts. However, for the purposes of evidence-based policy and programme development, it is important to acknowledge that there are differences between voluntary viewing of sexual content by children and viewing that is forced or coerced. The former is not included in the definition of OCSEA used in the *Disrupting Harm* study.

20. The only two legally binding international instruments containing an obligation to criminalise the grooming of children for sexual purposes are as follows: Council of Europe. (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Council of Europe Treaty Series – No. 201. Article 23; and European Parliament and Council. (2011). Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Article 6.
21. Cooper, K., Quayle, E., Jonsson, L. & Svedin, C.G. (2016). Adolescents and self-taken sexual images: A review of the literature. Computers in Human Behavior, vol. 55, 706-716.
22. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 52.
23. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International, 21.
24. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International, 44.

ABOUT MALAYSIA – DEMOGRAPHICS AND INTERNET USAGE

Despite increasing connectivity around the world, few countries regularly update their formal internet use statistics or disaggregate them for their child populations. This presents a challenge to understanding how young people's lives are impacted by digital technologies, particularly in low- and middle-income countries. The infographic below summarises the latest data on internet access and social media use in Malaysia; some of this data was gathered directly through the Disrupting Harm nationally representative household survey of internet-using 12–17-year-olds.

The data below provides an important backdrop for understanding the various facets of children's internet use. However, methodological limitations affecting data quality for certain secondary sources should be kept in mind. Relying on purposive or other non-probability sampling techniques means that the data cannot be considered representative of the population in question. In other cases, variations in the data collection methods and definitions of internet use pose a challenge for cross-country comparisons.

POPULATION TOTAL 2020

Country data:

32,447,385[25]

UN data:

32,366,000[26]

FEMALE POPULATION 2020

Country data:

15,481,168[27]

UN data:

15,735,000[28]

MALE POPULATION 2020

Country data:

16,966,217[29]

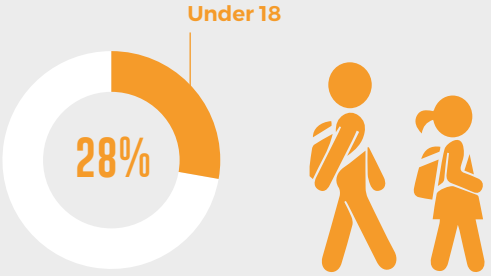
UN data:

16,631,000[30]

POPULATION UNDER 18 2020

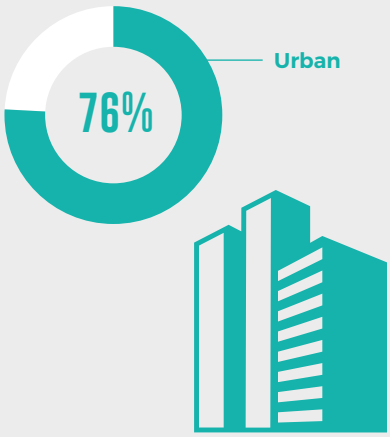
UN data:

9,162,000[31]



URBAN POPULATION 2018: 76%[32]

2030 prospective: 82%[33]



MEDIAN AGE 2020[34]

30.3

Estimate

GDP PER CAPITA 2020 (US$)

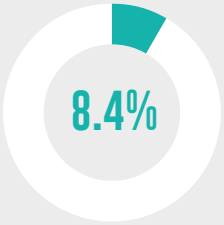
$10,412[35]

25. Department of Statistics Malaysia (2020). Key Findings Population and Housing Census of Malaysia 2020.
26. United Nations Population Division. (n.d.). World Population Prospects 2019.
27. Department of Statistics Malaysia (2020). Key Findings Population and Housing Census of Malaysia 2020.
28. United Nations Population Division. (n.d.). World Population Prospects 2019.
29. Department of Statistics Malaysia (2020). Key Findings Population and Housing Census of Malaysia 2020.
30. United Nations Population Division. (n.d.). World Population Prospects 2019.
31. UNICEF. (2021). The State of the World's Children 2021. UNICEF, New York.
32. United Nations Population Division. (n.d.). World Urbanization Prospects: The 2018 Revision.
33. United Nations Population Division. (2019). World Population Prospects 2019.
34. United Nations Population Division. (2019). World Population Prospects 2019 File POP/5: Median age by region, subregion and country, 1950-2100 (years).
35. World Bank. (2020). GDP per capita (current US$) - Malaysia.

ABOUT MALAYSIA – DEMOGRAPHICS AND INTERNET USAGE

POVERTY RATES

HEADCOUNT RATIO AT NATIONAL POVERTY LINES[36] (% OF POPULATION)

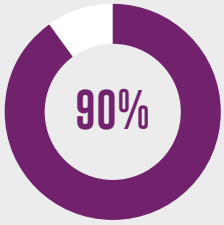


LANGUAGE

MALAY

(BAHASA MALAYSIA)[37]

INTERNET SUBSCRIPTION/PENETRATION RATES 2020: 90%[38]



INTERNET USE AMONG CAREGIVERS OF INTERNET-USING CHILDREN

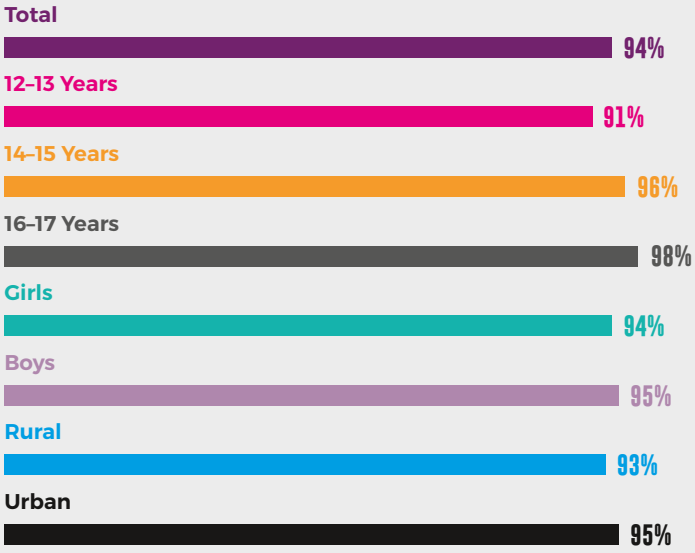
98%

Source: Disrupting Harm data

n = 995 caregivers of internet-using children.

2020 INTERNET PENETRATION RATES AMONG 12–17-YEAR-OLDS

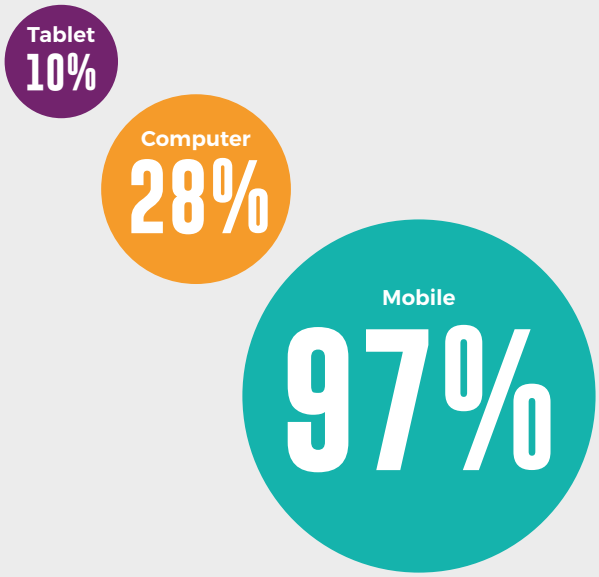
Source: Disrupting Harm data



n = 1,505 households.

MOST POPULAR DEVICE TO ACCESS THE INTERNET AMONG 12–17-YEAR-OLDS*

Source: Disrupting Harm data



n = 995 internet-using children.

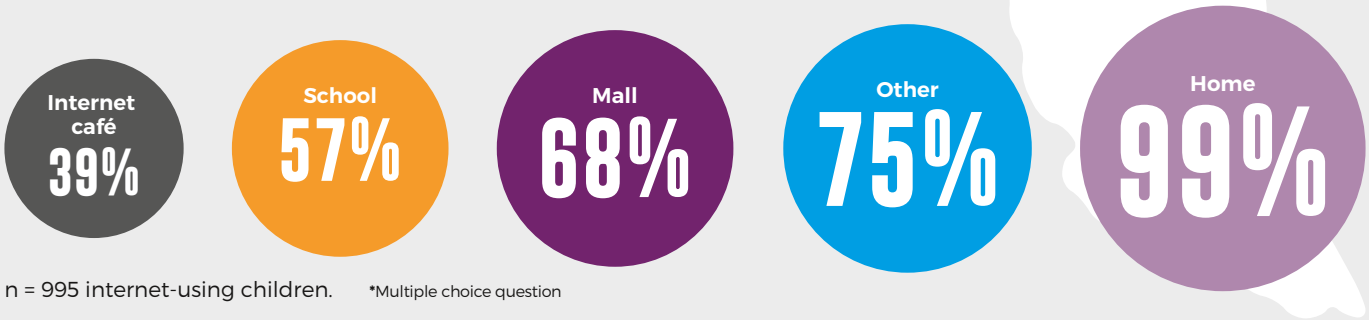
*Multiple choice question

36. World Bank. (n.d.). Poverty & Equity Data Portal.
37. Government of Malaysia. (1957). Federal Constitution of Malaysia (Perlembagaan Persekutuan Malaysia), Section 152(1).
38. International Telecommunications Union. (2020). Country ICT data: Percentage of Individuals Using the Internet.

ABOUT MALAYSIA – DEMOGRAPHICS AND INTERNET USAGE

MOST POPULAR PLACE TO ACCESS THE INTERNET AMONG 12–17-YEAR-OLDS*

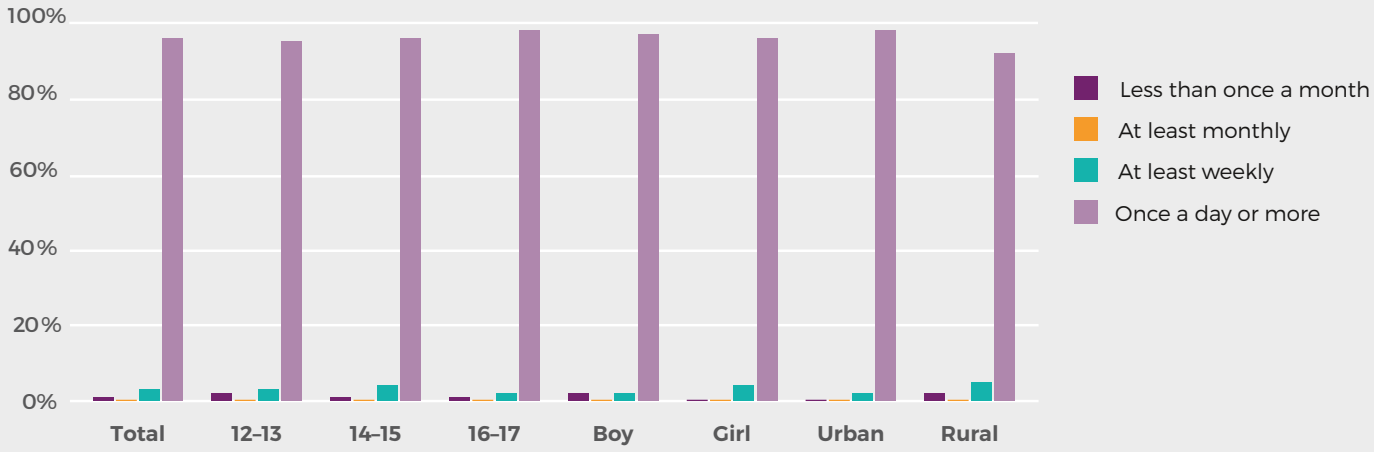
Source: Disrupting Harm data



n = 995 internet-using children. *Multiple choice question

FREQUENCY OF INTERNET USE AMONG 12–17-YEAR-OLDS

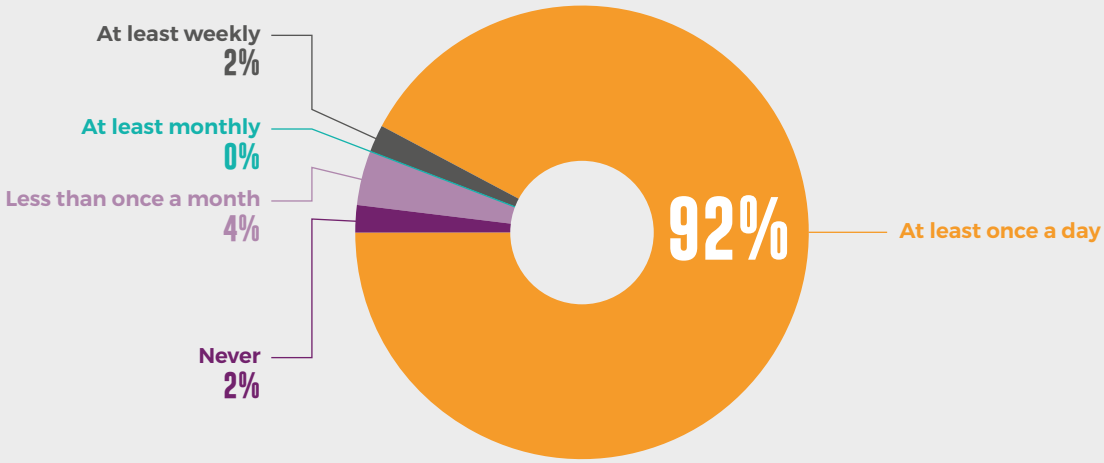
Source: Disrupting Harm data



Base: Internet-using children aged 12–17 in Malaysia from the Disrupting Harm study. n = 995.

FREQUENCY OF INTERNET USE AMONG CAREGIVERS OF INTERNET-USING CHILDREN

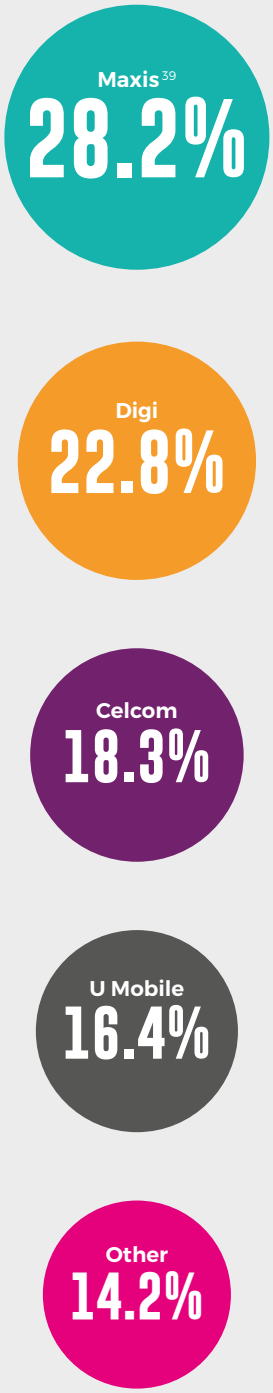
Source: Disrupting Harm data



n = 995 caregivers of internet-using children.

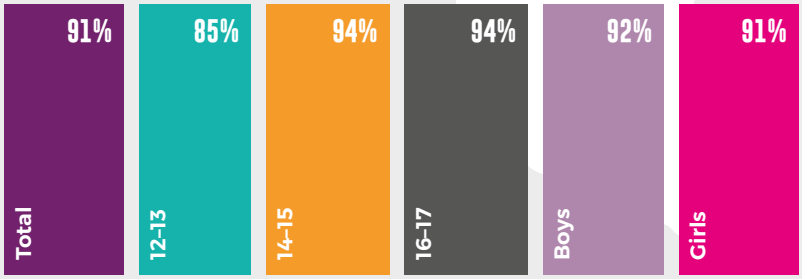
ABOUT MALAYSIA – DEMOGRAPHICS AND INTERNET USAGE

MARKET SHARES IN MOBILE DATA SUBSCRIPTIONS (2020)



CHILDREN WHO USE SOCIAL MEDIA ON A WEEKLY BASIS

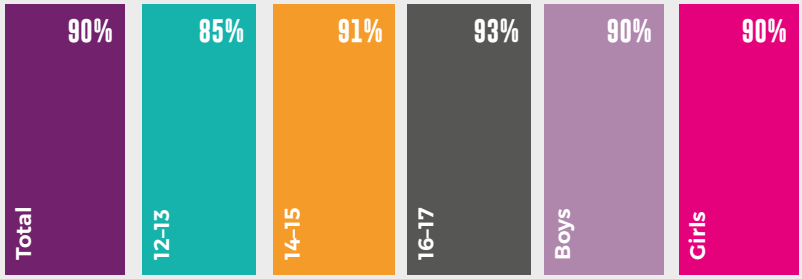
Source: Disrupting Harm data



n = 995 internet-using children aged 12–17.

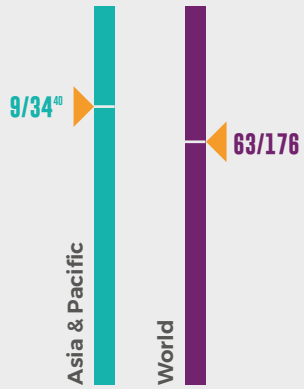
CHILDREN WHO USE INSTANT MESSAGING APPS ON A WEEKLY BASIS

Source: Disrupting Harm data



n = 995 internet-using children aged 12–17.

ICT DEVELOPMENT INDEX RANKING (ITU) 2017



GLOBAL CYBERSECURITY INDEX RANKING 2018[41]

39. Malaysian Communications and Multimedia Commission (2020). Industry Performance Report 2020.
40. International Telecommunication Union. (2017). ICT Development Index 2017.
41. The Global Cybersecurity Index measures the commitment of countries to cybersecurity based on the implementation of legal instruments and the level of technical and organisational measures taken to reinforce international cooperation and cybersecurity.
42. International Telecommunication Union. (2019). Global Cybersecurity Index (GCI) 2018.

OVERVIEW OF LEGISLATION AND POLICY

In 2017, Malaysia took a progressive step in the protection of children from online sexual exploitation and abuse by enacting the Sexual Offences against Children Act.[43] One government representative was of the view that the *"Richard Huckle [case]44 triggered the enactment of Sexual Offences against the Children Act 2017."* (RA1-MY-11-A)

This act defines child sexual abuse material as "any representation in whole or in part, whether visual, audio or written or the combination of visual, audio or written, by any means including but not limited to electronic, mechanical, digital, optical or magnetic means, or manually crafted, or the combination of any means – (i) of a child engaged in sexually explicit conduct; (ii) of a person appearing to be a child engaged in sexually explicit conduct; (iii) of realistic or graphic images of a child engaged in sexually explicit conduct; or (iv) of realistic or graphic images of a person appearing to be a child engaged in sexually explicit conduct".[45] This definition comprehensively covers visual, audio and written materials, and digitally generated child sexual abuse material and materials that depict a person appearing to be a minor engaged in sexually explicit conduct. The definition further includes materials showing the sexual parts of a child for primarily sexual purposes,[46] as recommend by the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.[47]

The Sexual Offences Act prohibits a wide range of acts related to CSAM, such as using a child or causing a child to be used in the production of these materials,[48] and making, producing and directing the making or production of CSAM.[49] Taking any action in preparation for the production of CSAM is also criminalised.[50] Moreover, the legislation criminalises the act of distributing, promoting, importing, exporting, selling,[51] knowingly accessing and possessing CSAM.[52]

Aside from these CSAM-specific provisions, the Penal Code bans the publication, sale, possession and showing of and acting in obscene materials and exhibitions. Although not explicitly indicated, this ban would encompass pornography (including materials and shows depicting adults).[53]

The Sexual Offences against Children Act also criminalises the act of sexually communicating with a child or encouraging a child to sexually communicate by any means.[54] The broad wording of this provision suggests that it could be used to address grooming in the online context. The term 'sexually communicating' is understood when "(a) the communication or any part of the communication relates to an activity that is sexual in nature; or (b) any reasonable person would consider any part of the communication to be sexual."[55]

43. Government of Malaysia. (2017).Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017.
44. Richard Huckle was a British national convicted in 2016 for sexually abusing up to 200 Malaysian children over an eight-year period during his time volunteering at orphanages in the country. Questions regarding why it took so long for him to be brought to justice are thought to have spurred efforts in Malaysia to address CSEA and OCSEA issues more proactively. Paedophile Richard Huckle, Who Targeted Poor Malaysian Children, Faces Life In Prison | HuffPost UK News (huffingtonpost.co.uk).
45. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 4.
46. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 4 (b) (v).
47. United Nations General Assembly. (2000). Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. A/RES/54/263 of 25 May 2000 entered into force on 18 January 2002. Article 2(c).
48. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 7.
49. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 5.
50. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 6.
51. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 8–9.
52. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 8–9.
53. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Section 292.
54. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section. 11.
55. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 11 (2).

Additionally, the law makes it an offence for anyone to communicate with a child with the intention of committing or facilitating offences related to CSAM or sexual abuse.[56] In the latter case, the penalty of imprisonment would be increased from five years (for sexually communicating with the child) to 10 years.[57]

Although Malaysian legislation does not explicitly criminalise the live-streaming of child sexual abuse, aside from a prohibition to recruit children for pornographic performances,[58] interviews conducted by *Disrupting Harm* indicated that persons committing this crime could be charged under existing provisions on CSAM.

The majority of interviewees were of the view that the existing laws are sufficient to protect children from OCSEA. Despite this, the law enforcement data shows that registered cases of OCSEA are uncommon. Representatives of the Legal Affairs Division of the Prime Minister's Department noted that government agencies have made no progress in terms of evaluating the implementation of the Sexual Offences against Children Act as there has been no engagement with other agencies on the act since it was passed. (RA1-MY-04-A, B &C)

Inconsistencies exist, for example, under the Penal Code, statutory rape – denoted as penetrative sexual intercourse – is only applied to girls below the age of 16.[59] The age of consent for non-penetrative sexual acts, which falls under the Penal Code's "acts of gross indecency", is set at 14 for all children,[60]while the provisions of the Sexual Offences against Children Act apply to all children below the age of 18. In practice, such inconsistencies may lead to different levels of protection depending on the sex and age of the children involved in the abuse. Girls aged between 16 and 18 and boys of all ages may be less protected when adults victimise them. The minimum age of criminal responsibility in Malaysia is 10 years old,[61] meaning that boys may be at risk of being criminalised for consensual sex with same-aged female peers. Another provision which, although not specific to OCSEA, can have an impact on the reporting and prosecution of these crimes is the prohibition of male homosexual relations, which is currently criminalised as acts "against the order of nature" in the Malaysian Penal Code.[62]

Malaysia has adopted four national plans of action related to child protection and child development, namely, the 2009 National Child Protection Policy,[63] the 2009 National Child Policy, the National Plan of Action on Trafficking in Persons (2016–2020) and the Plan of Action on Child Online Protection (2015–2020).

56. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 13.
57. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Sections 11 and 13.
58. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 7.
59. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Section 375.
60. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Section 377E.
61. Nevertheless, a person above 10 years old and under 12 years old who has not attained sufficient maturity of understanding to judge the nature and consequence of their conduct is not liable for any offence. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Sections 82 and 83.
62. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Sections 377A and 377B.
63. Mohd, A. & Kadir, N. (2012). Protection of Children in Malaysia through Foster Care Legislation and Policy. *Australian Journal of Basic and Applied Sciences*. 6. 113–118.

The Plan of Action on Child Online Protection (2015–2020) was approved in February 2015 and includes 20 strategies regarding advocacy, awareness-raising, prevention, intervention and support services. Several government agencies were involved in the implementation of this plan, in collaboration with non-governmental organisations.[64,65] A high-level review on the Plan of Action on Child Online Protection (2015–2020) is currently being undertaken as part of the development of the new National Child Policy by Ministry of Women, Family and Community Development, supported by UNICEF in collaboration with a technical working group that includes the Malaysian Communications and Multimedia Commission, the Office of Children's Commissioner (SUHAKAM) and other stakeholders. One government representative interviewed by *Disrupting Harm* commented that, despite its development on paper, the Plan of Action was not effectively implemented and had little impact in tackling OCSEA. (RA1-MY-03-A &B)

Government representatives noted that the main challenges facing government agencies in the implementation of such policies were related to limited financial resources and a lack of trained personnel. It was indicated that, in general, the various policies related to child protection and child development are not adequately incorporated into government decisions.

At a regional level, Malaysia, as a member of the Association of Southeast Asian Nations (ASEAN), is committed to the ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016–2025. During the 35th ASEAN Summit in November 2019, Malaysia committed itself to the Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN.

“Government representatives noted that the main challenges facing government agencies in the implementation of policies were related to limited financial resources and a lack of trained personnel.”

64. Internet Society (2017). Mapping Online Child Safety in Asia Pacific.
65. Malaysian Communications and Multimedia Commission (2016). Implementing Child Online Protection (COP) Plan Presentation.

1. CHILDREN ONLINE IN MALAYSIA

The main focus of the *Disrupting Harm* report series is to present the perspectives of young people, government representatives, service providers and others with a role in combating the sexual exploitation and abuse of children facilitated or committed through digital technologies. However, it is important to situate these offences within the wider context of children's internet use in Malaysia. This first chapter, therefore, presents a brief overview of children's internet access and the activities enjoyed by the majority of children online before going on to describe the occurrence of riskier online activities and the ways in which these are perceived by internet-using children and their caregivers.[66]

66. In the household survey, the term "caregiver" is an inclusive term used to refer to all those adults who are responsible for children such as parents, step-parents, grand-parents or other legal guardians.

1.1 INTERNET ACCESS AND BARRIERS

Children's access: Sampling data from the *Disrupting Harm* household survey suggests that 94% of 12–17-year-olds in Malaysia are internet users, i.e., they have used the internet within the past three months. Children aged 16–17 were somewhat more likely to be internet users (98%) than children aged 12–13 (91%). Boys and girls, and rural and urban children, were equally likely to be internet users.[67,68]

Ninety-six percent of children, with no variations according to age, gender or their location in rural or urban areas, go online at least once a day (see Figure 3). Indeed, Malaysia has one of the highest internet penetration rates in Southeast Asia, second only to Singapore.[69]

Caregivers' access: One caregiver of each child interviewed also took part in the survey. Most caregivers were at least daily internet users themselves. The sampling data showed that slightly more caregivers of internet-using children (98%) were online as compared to the children (94%) – an uncommon finding in *Disrupting Harm* countries in which children were more often online. only 2% of the caregivers had never been online, though this was more pronounced in the caregivers aged 50 and above (7%). The proportion of caregivers who use the internet daily was slightly lower in rural areas than in urban areas (rural: 88%; urban: 94%) (see Figure 4).

Devices used: As in most other countries, smartphones were by far the most common device used by 12–17-year-old internet users to go online, probably due to their relatively low cost and portability.[70] Ninety-seven percent of the children surveyed used smartphones, while 28% used computers and 10% used tablets. The use of computers (rural: 9%; urban: 36%) and tablets (rural: 6%; urban: 12%) was higher among children living in urban areas than children living in rural areas. Higher rates of computer use among urban children may be related to socio-economic status, whereby certain urban households own both phones and computers.

It may also relate to the activities children engage in online, e.g., urban children may be more likely to use the internet to do schoolwork and play online games than their rural counterparts (see chapter 1.2). There were no notable differences according to age or gender in terms of devices used.

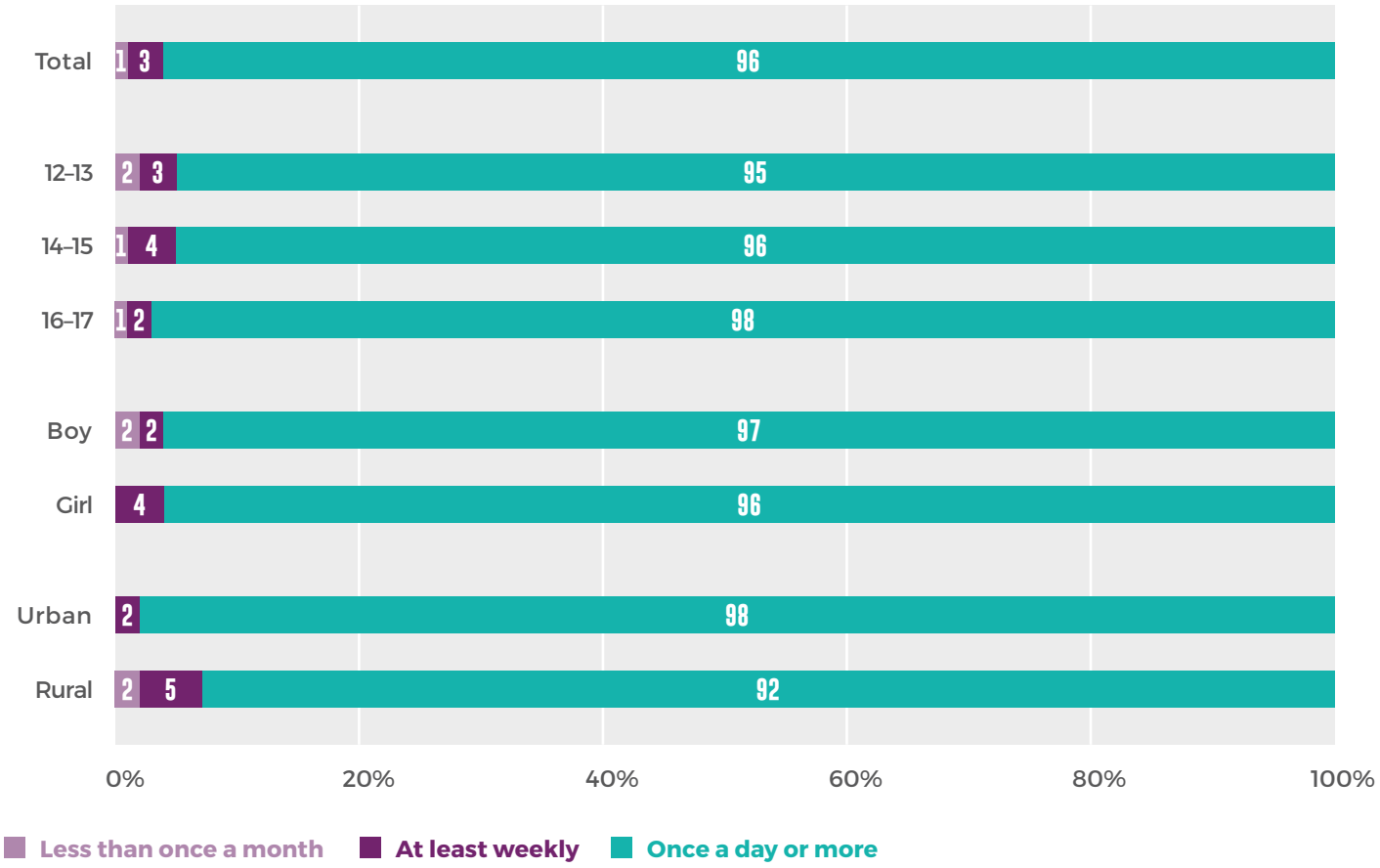
Of the children who used a smartphone, only 25% shared it with someone else: a lower proportion than in many other *Disrupting Harm* countries. The proportion of internet-using children who shared their smartphones with others ranged from 13% among children aged 16–17 to 44% among 12–13-year-olds. Children mainly shared their mobile or smartphones with caregivers (16%) or siblings (13%). Sharing devices could have implications in terms of a children's ability to control the security of their profiles or other internet access.

Place of access: Almost all the 12–17-year-old internet users who took part in the household survey (99%) accessed the internet at home, and 57% accessed the internet at school. However, only 19% of children went online at school every day, possibly due to COVID-19-related school closures. Younger children, aged 12–13, were slightly less likely to access the internet at school on a daily basis than 16–17-year-olds (19% versus 24%). Children living in urban areas were more likely to go online at school than children living in rural areas (rural: 42%; urban: 63%).

Some of the children surveyed also accessed the internet via public networks at malls (68%) and internet cafes (39%), but few children said they did so every day (6% and 4% respectively). Seventy-five percent of children said they went online from a place that was not captured in the survey, which might mean the street, a friend's house or the park, for example.

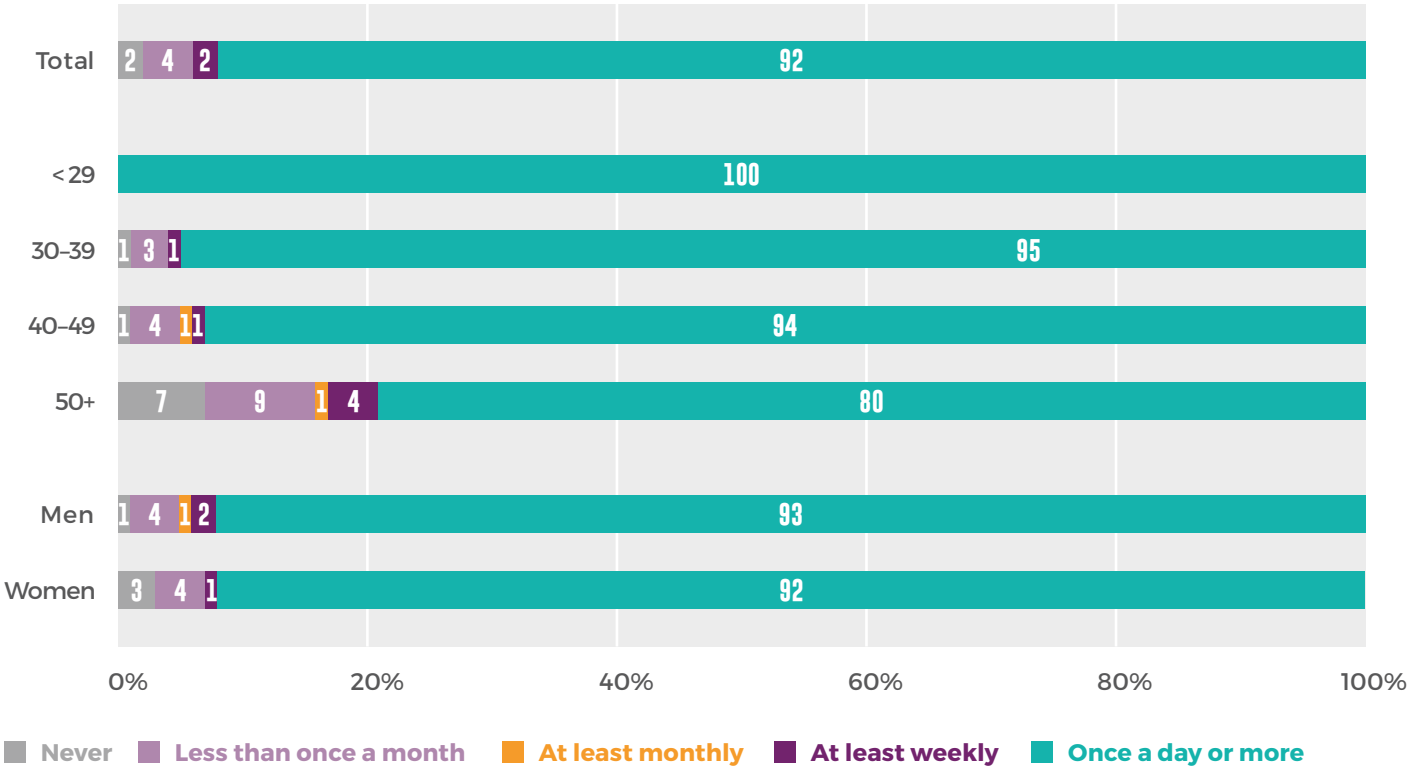
67. During the random walk to identify eligible children to take part in the main survey, data was also collected from every household visited about the number of 12–17-year-old children living there, their gender, age and whether they had used the internet in the past three months. This made it possible to estimate internet penetration rates for all the 12–17-year-old children in Malaysia. n = [x] households.
68. The question used to determine whether a 12–17-year-old was an internet user was as follows: Has [PERSON] used the internet in the last three months? This could include using a mobile phone, tablet or computer to send or receive messages, use apps like Facebook, WhatsApp or Instagram, send emails, browse, chat with friends and family, upload or download files, or anything else that you usually do on the internet.
69. World Bank Group and Ministry of Finance (2018). Malaysia's Digital Economy. A New driver of Development.
70. Kardefelt Winther, D., Livingstone, S., & Saeed, M. (2019). Growing up in a connected world. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

Figure 3: Frequency of children's internet use (%).



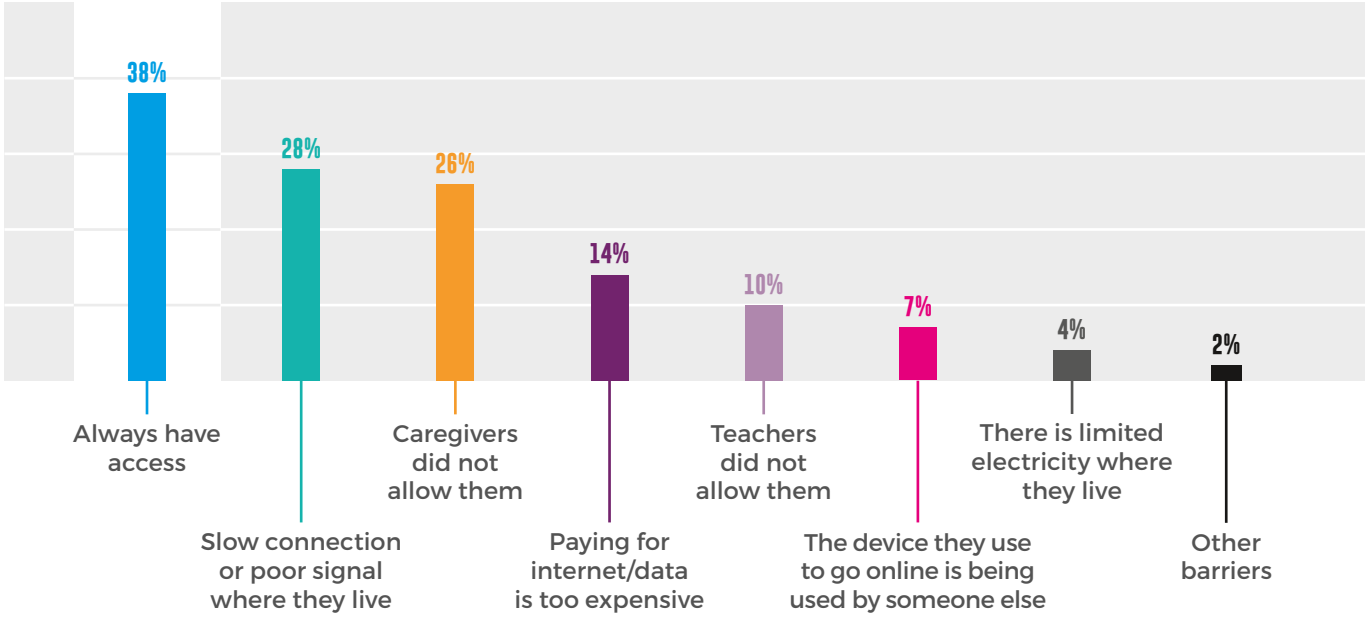
Base: Internet-using children aged 12–17 in Malaysia. n = 995.

Figure 4: Frequency of caregivers' internet use (%).



Base: Caregivers of Internet-using children aged 12–17 in Malaysia. n = 995.

Figure 5: Barriers to access for internet-using children.



Base: Internet-using children aged 12–17 in Malaysia. n = 995.

Barriers to access: A majority (62%) of internet-using 12–17-year-olds in Malaysia face barriers in terms of accessing the internet when they want or need it (see Figure 5). Children in urban areas were more likely to report that they always have access to the internet than their rural counterparts (42% versus 28%). A slow connection or poor signal was the most commonly cited reason for limited access, affecting 28% of children.

> **While a restrictive approach might reduce children's exposure to online risks in the short term, it also reduces their familiarity with the online environment in the long term. Moreover, children might view restrictions as a form of punishment, and be deterred from voicing their concerns about unwanted experiences online.**

Children in rural areas were over twice as likely than children in urban areas to cite a poor signal as a barrier to access (45% versus 21%). Older children aged 16–17 also cited this barrier more often than younger children (12–13: 24%; 16–17: 32%). This may relate to the nature and range of activities older children engage in online (see chapter 1.2).

Children also reported restrictions to internet access imposed by their caregivers. A higher percentage of younger children cited parental restrictions as a barrier to access (12–13: 38%; 14–15: 25%; 16–17: 16%).

While a restrictive approach might reduce children's exposure to online risks in the short term, it also reduces their familiarity with the online environment in the long term. Moreover, children might view restrictions as a form of punishment, and be deterred from voicing their concerns about unwanted experiences online. Some level of parental restrictions may be protective if overall caregiver engagement with children centres around guidance and support in case they encounter harm online (see page 36 for more on parental support).

1.2 CHILDREN'S ACTIVITIES ONLINE

Approximately nine out of 10 of the surveyed children reported that they commonly used social media (91%), took part in instant messaging (90%) and watched video clips (88%) on a weekly basis (see Figure 6). The vast majority also used the internet for schoolwork (86%). Other popular activities included talking to family or friends who live far away (73%), watching a livestream (72%) and playing video games (72%).

The older children were particularly likely to engage in most activities, including the use of social media and instant messaging, on a weekly basis. No significant gender differences were observed in children's activities online except for gaming, which was much more common among boys (84% played games at least once a week) than girls (59%) – a trend also observed in other *Disrupting Harm* countries.

Research on gender differences in the use of online games indicates that gaming continues to be dominated by male players, who are more motivated to play, start playing games earlier in life, play more frequently and spend more time playing. Evidence shows that men and women prefer different types of games and engage in different types of activities while gaming.[71,72]

Figure 6: Activities children engage in online at least once a week.

Children's online activities	Total	12–13	14–15	16–17	Boy	Girl	Urban	Rural
Used social media	91%	85%	94%	94%	92%	91%	93%	88%
Used instant messaging	90%	85%	91%	93%	90%	90%	91%	88%
Watched videos	88%	85%	89%	90%	87%	89%	91%	82%
Schoolwork	86%	87%	86%	86%	87%	86%	88%	83%
Talked to family or friends who live further away	73%	73%	74%	71%	72%	73%	74%	70%
Played online games	72%	74%	71%	71%	84%	59%	76%	63%
Watched a livestream	72%	69%	69%	76%	73%	70%	75%	64%
Searched for new information	60%	55%	58%	68%	60%	60%	65%	48%
Looked for information about work or study opportunities	53%	54%	52%	53%	49%	57%	58%	42%
Participated in a site where people share their interests/hobbies	40%	38%	37%	46%	43%	38%	44%	32%
Followed celebrities or public figures on social media	41%	38%	38%	45%	40%	42%	45%	32%
Looked for news	37%	33%	32%	45%	39%	35%	42%	24%
Looked for health information	30%	31%	28%	31%	28%	32%	36%	17%
Sought emotional support	28%	29%	27%	28%	26%	30%	32%	19%
Created their own video or music	20%	22%	19%	21%	20%	21%	22%	17%
Looked for information or events in local neighbourhood	21%	22%	21%	22%	21%	22%	25%	14%
Discussed political or social problems	15%	15%	14%	16%	15%	15%	17%	10%
Created a blog or website	14%	15%	12%	15%	14%	14%	16%	11%

Internet-using children aged 12–17 in Malaysia. n = 995.

71. Veltri et al. (2014). Gender Differences in Online Gaming: A Literature Review.
72. Leonhardt, M.; Overå, S. (2021). Are There Differences in Video Gaming and Use of Social Media among Boys and Girls?—A Mixed Methods Approach. Int. J. Environ. Res. Public Health, 18, 6085.

1.2 CHILDREN'S ACTIVITIES ONLINE

The survey data also suggests that children living in rural areas engage in all activities to a lesser extent than children living in urban areas. While few differences were observed for activities relating to communication (the use of social media or instant messaging, for instance), children in rural areas were less likely to use the internet at least once a week for entertainment activities and to seek information than their urban peers. For example, only 48% of rural children used the internet at least once a week to look for new information (as compared to 65% of urban children) and only 17% looked for health information online (as compared to 36% of urban children).

The categories used in the survey are not mutually exclusive. For example, a child could go online to watch a video as part of their schoolwork. Nonetheless, Figure 6 provides a greater understanding of how 12–17-year-olds in Malaysia use the internet and the activities they enjoy.

> **Approximately nine out of 10 of the surveyed children reported that they commonly used social media (91%), took part in instant messaging (90%) and watched videoclips (88%) on a weekly basis. The vast majority also used the internet for schoolwork (86%).**

1.3 PERCEPTIONS AND EXPERIENCES OF RISKY ONLINE ACTIVITIES

Discussions concerning online risks often hinge upon adult-centric perceptions. To help us understand children's perceptions, they and their caregivers were asked about their engagement in, and perceptions of, various risky online activities.

1.3.1 Contact with strangers online and in person

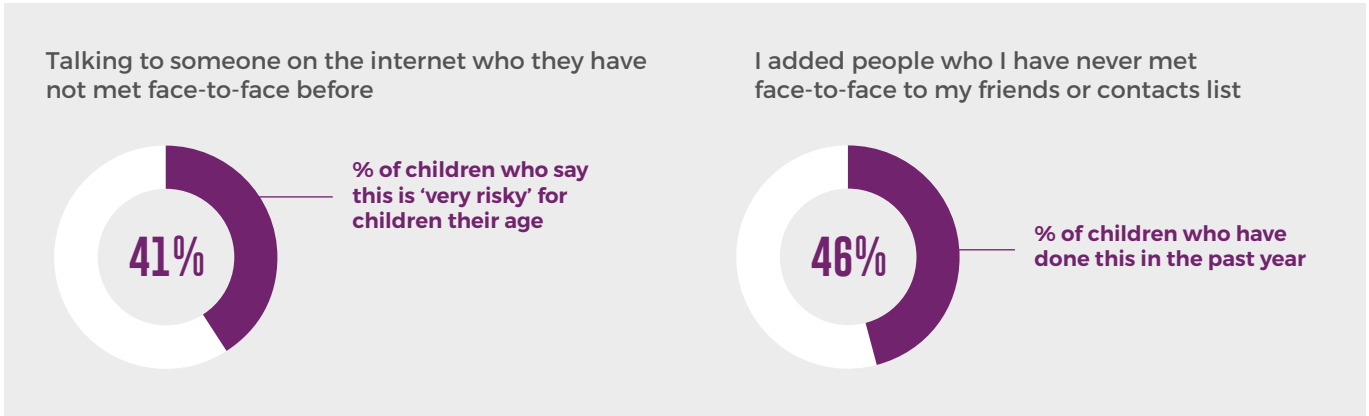
Communicating with strangers online

A common concern around children's online use is their exposure to 'stranger danger'. In the household survey, 62% of the caregivers rated "talking to someone on the internet who they have not met face-to-face before" as 'very risky' for children. Yet, only 41% of the children rated this activity as 'very risky' for children of their age. Children aged 12–15, and girls, were most likely to describe talking online with a person they did not know as 'very risky'. Similarly, 84% of the caregivers surveyed thought it 'very risky' for children to send their personal information to someone they had never met face-to-face, as compared to 71% of the children (again, particularly girls). Among the caregivers, these risk perceptions increased with age.

While most of the internet-using children recognised that interacting online with unknown people carries some level of risk, 14% felt that there was no risk at all. While generally such interactions do not cause harm and are simply a way for young people to make new friends, this response signals a lack of awareness among some children about how speaking to strangers online can lead to harmful outcomes. One survivor of OCSEA in Malaysia explained how she began communicating with unknown people online: *"When Mum was at work, I would hold the phone and that's when I would watch and read Mum's messages with that man on her WhatsApp and WeChat. So I felt OK then, if Mum can do it, so can I.... Even with this Omegle, 73 I did it behind her back, without her knowledge so with them, yes, it is my fault because I still did it even though I knew it was wrong. She said she didn't know how else to guide me ...."* (RA5-MY-02)

In practice, a considerable proportion of children do engage with 'online strangers'. For example, 46% of children said they had added people they had never met face-to-face to their contact lists in the past year. This figure ranged from 33% for 12–13-year-olds to 51% for 16–17-year-olds. There was no notable difference according to gender.

Figure 7: Level of risk attributed by children to speaking to someone unknown online.



Base: Internet-using children aged 12–17 in Malaysia. n = 995

73. Omegle is a free online chat website that allows users to socialise with others without the need to register. The service randomly pairs users in one-on-one chat sessions where they chat anonymously.

Figure 8: Level of risk attributed by children to sharing personal information with unknown people online.

Base: Internet-using children aged 12–17 in Malaysia. n = 995

Meeting someone in person following an online interaction

In the household survey, 63% of the children and 77% of their caregivers – particularly female caregivers and caregivers in urban areas – rated "going to meet someone face-to-face that they first got to know online" as 'very risky' for children. More girls than boys regarded this as high-risk behaviour (70% versus 56%). However, 7% of children viewed this behaviour as 'not risky at all'.

There are clearly incongruences between the perceptions of children and their caregivers. Meeting someone you do not know face-to-face for the first time can be very risky. This report refers to various cases that had severe consequences. One young person interviewed in Malaysia was 13 years old when she met someone in person that she had first met online via Facebook Messenger. She described how they 'dated' online and how he requested sexual pictures of her: *"Yeah, you know like show me your body and things like that. Yeah. And then he did ask me to send him nudes. At that time, I wasn't sure if this is right, but I did send and after that, when he used to ask, I was like, 'Oh, no, no' and then he forced me to send. He said he would break up with me. And then I felt bad, I felt sad because I loved being with him".*

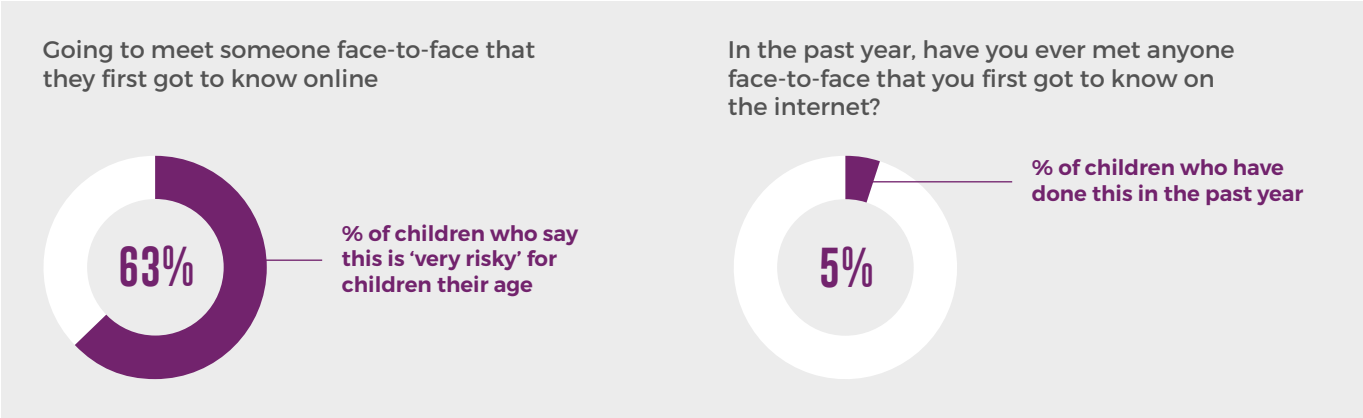
She agreed to meet him and, at first, he was nice to her and told her how pretty she was; however, this changed very quickly, and she was sexually assaulted.

Such worst-case scenarios probably explain why caregivers are so worried about their children's online interactions. However, the outcomes of face-to-face encounters between children and persons they have got to know online depend on the context and purpose, e.g., connecting with new children from school or the community first online and then in person, or going to group events with caregivers is different from going alone to meet someone completely unknown.

In Malaysia, 5% of the children surveyed had met someone in person whom they had first met online in the previous year. Among the children who had face-to-face encounters with persons they had first met online, the great majority reported that they were happy or excited about the experience (see Figure 10). Research from across more than 30 countries around the world has produced similar findings.[74,75]

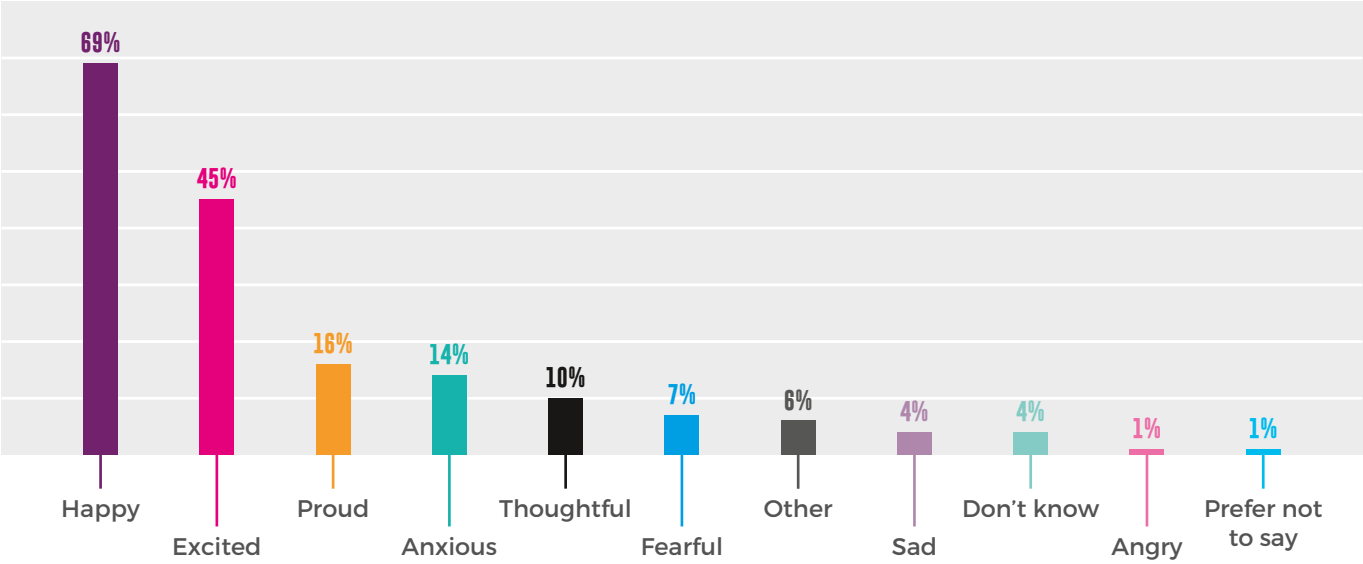
74. Smahel, D., Machackova, H., et al. (2020). EU Kids Online 2020: Survey results from 19 countries. Florence: UNICEF Office of Research – Innocenti.
75. Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

Figure 9: Level of risk attributed by children to meeting someone in person who they first met online.



Base: Internet-using children aged 12–17 in Malaysia. n = 995

Figure 10: How children felt the last time they met someone face-to-face whom they had first got to know on the internet.



Base: Children who, within the past year, have met someone face-to-face who they first got to know on the internet. n = 995.

Empowering Caregivers to Guide their Children's Internet Use

Caregivers can be a first line of defence in protecting children from online harm – particularly if they have a grasp of basic digital skills and activities, are aware of online risks, avoid restrictions or punitive responses and focus on helping and supporting their children to stay safe online.

In Malaysia, caregivers use the internet at higher rates than their children – an uncommon finding among the *Disrupting Harm* countries in Southeast Asia, which demonstrates that Malaysia is particularly advanced with respect to digital diffusion. However, there does remain an age divide in terms of internet use and digital skills, with older caregivers at a disadvantage when compared to their younger peers. Seven percent of the caregivers aged 50 or above included in the household survey had never used the internet and only 80% used it on a daily basis. These caregivers also had the weakest digital skills. For example, only 44% said they knew how to report harmful content on social media, as compared to 87% of caregivers aged 29 or younger.

'Family and Communication Technology' was the domain of family wellbeing that obtained the second lowest score (6.38 out of 10) in the Malaysia Family Wellbeing Index in 2016. This indicates a need to instil awareness on the issue of child online protection among parents in Malaysia and to equip them with useful digital parental know-how.[76]

"As with all countries, things can be improved further. Adults (not just parents and caregivers) need to be equipped with digital parenting, literacy and resilience skills." (RA3-MY-16-A)

When faced with constant reports that greater access to technology and the internet can increase children's vulnerability to OCSEA – a view shared by 47 out of the 50 service providers surveyed for *Disrupting Harm* – caregivers might instinctively react by restricting their children's internet use in a bid to protect them. In the household survey, 36% of the caregivers said they would restrict their child's internet access if their child was bothered by something online. Interestingly, it was the youngest caregivers, aged 29 or younger, who were most likely to give this response (43%, as compared to 35% of caregivers older than 50).

While a restrictive approach might reduce children's exposure to online risks in the short term, it also risks reducing their digital skills and familiarity with the online environment in the long term. Furthermore, it is plausible that, as these restrictions disconnect children from their online lives completely, such a response will be viewed as a form of punishment. This could make children less likely to voice concerns about harm or other unwanted experiences they encounter online.

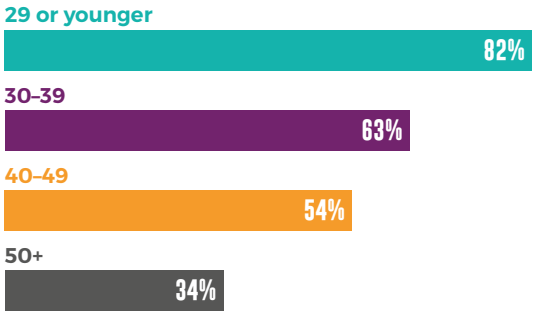
Focus group discussions conducted by DiGi Telecommunications and Kantar TNS among students aged 13–16 in Malaysia in 2017 showed that many children did not seek help after experiencing cyberbullying, and that they appeared to conceal such incidents from their parents for fear of closer supervision and control, out of concerns that they would not be heard and worries about losing pride. This was particularly true of boys.[77]

76. National Population and Family Development Board (LPPKN) (2016). Malaysia Family Wellbeing Index 2016.
77. Kantar TNS (2017). Project Safeguard. CyberSAFE.

On the other hand, *supportive engagement* by adults has been associated with positive digital skills development for children in other countries.[78] This includes engaging in activities together, talking to children about their internet use and educating them about the risks that exist online and how best to mitigate them. Engaging with children in this way allows them to reap the benefits of the many useful activities and skills that the internet has to offer while providing parental guidance and support in case they encounter any kind of harm online.

It is, therefore, encouraging that a majority of children in Malaysia say that their caregivers support their internet use. For example, 88% of the children surveyed said their caregivers suggest ways for them to stay safe online and 79% said their caregivers help them if they are bothered by something on the internet.

Figure 11: Caregivers who say they know more about the internet than their child, by age.



Base: Internet-using children aged 12–17 in Malaysia. n = 995.

According to *Disrupting Harm* data, on average, only 55% of caregivers in Malaysia said they knew more about the internet than their child, with stark differences between age groups (Figure 11). While 33% of caregivers felt they could help their children cope with things that bother them online 'a fair amount', one in five believed they could not help very much, if at all. It is possible that caregivers in Malaysia underestimate the extent to which they can help and support children.

Caregivers who are not internet users or who go online less frequently than their children might worry that they do not have enough knowledge to guide them. However, they can still talk to their children about what they do online and provide an open and supportive home environment where children feel comfortable talking about their online hobbies and interests or disclosing negative experiences. Among the caregivers surveyed, 63% said they would talk to their child if something bothered them online. It is important to provide these caregivers in particular with the knowledge and support they need to do this. Schools and parental education programmes can play an important role in this area. Helplines may also have a role to play as an information resource to caregivers.

As 64% of the children in the household survey considered their parents to be the persons most responsible for their online safety (after themselves), there is a need to equip caregivers with the skills and knowledge they need to help their children navigate online risks and to respond to online harms they may encounter.

78. Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

1.3.2. Seeing sexual images online

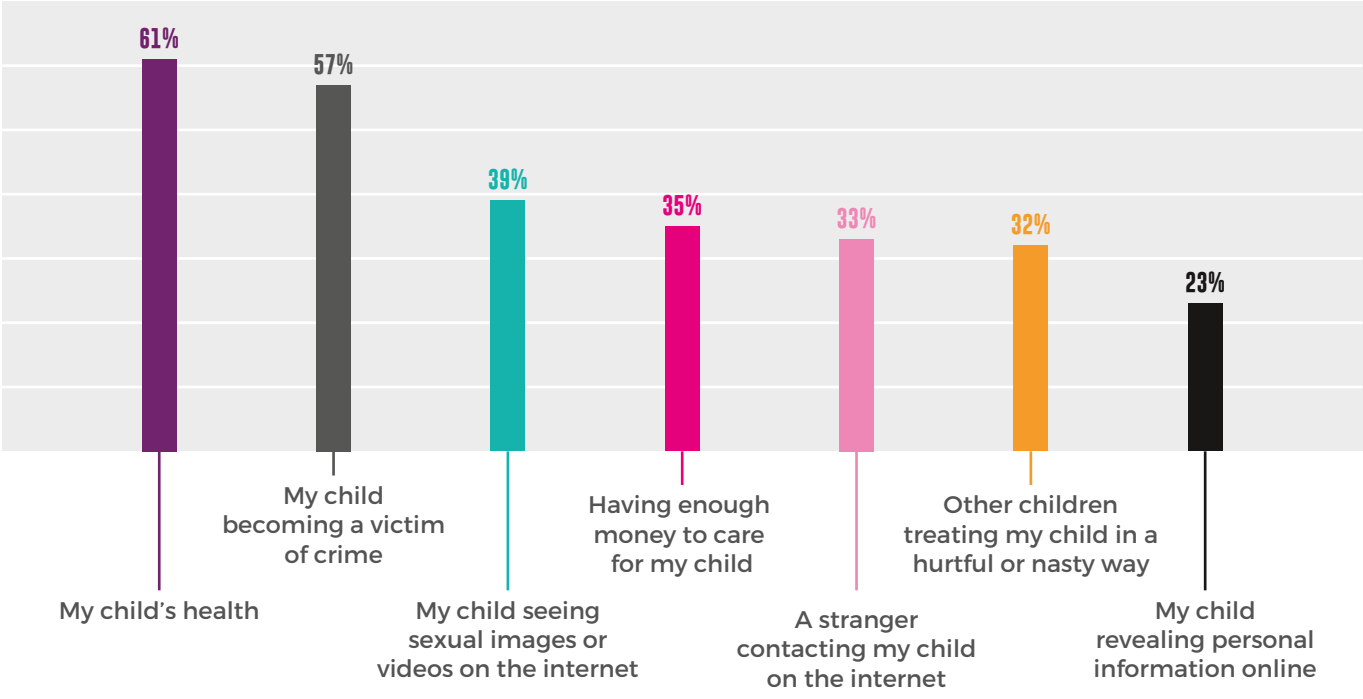
Seeing sexual content is the most important concern caregivers have about internet-related risks for their children.

Eighty-three percent of the caregivers, as well as 66% of the children surveyed, considered that children seeing sexual images or videos online was 'very risky' for children – higher percentages than for those who considered it 'very risky' to meet an online acquaintance face-to-face. Unlike in many other *Disrupting Harm* countries, these percentages were lower than the proportions of caregivers and children who found it 'very risky' to share personal information with a stranger online or to talk about sex with someone online. In absolute terms, the tendency to consider seeing sexual images or videos online 'very risky' was stronger in Malaysia than in several other countries, given that children and caregivers in Malaysia considered *all* the activities mentioned 'very risky' in larger proportions than in a number of other *Disrupting Harm* countries.

This concern around children seeing sexual images or videos, and around talking about sex with someone online, may reflect a prevalent discomfort concerning open discussion about sex and sexuality in Malaysia (see chapter 2.4). Ninety-six percent of the frontline workers surveyed as part of *Disrupting Harm* regarded 'access and exposure to pornography' as a factor that increases children's vulnerability to OCSEA, ahead of issues such as migration, experiences of family and community violence or living on the street (see Figure 13).

The different ways children see sexual content online can have different implications. Accidental or intentional glimpses of sexual content are one thing, being exposed to sexual images as part of a grooming process intended to desensitise the child and pave the way for subsequent requests for images or sexual acts (see chapter 2) is another. While viewing violent or degrading sexual content can serve to normalise harmful gender norms and sexual behaviour, seeing pornography online appears to be an increasingly common experience for young people. Both phenomena need to be addressed.[79]

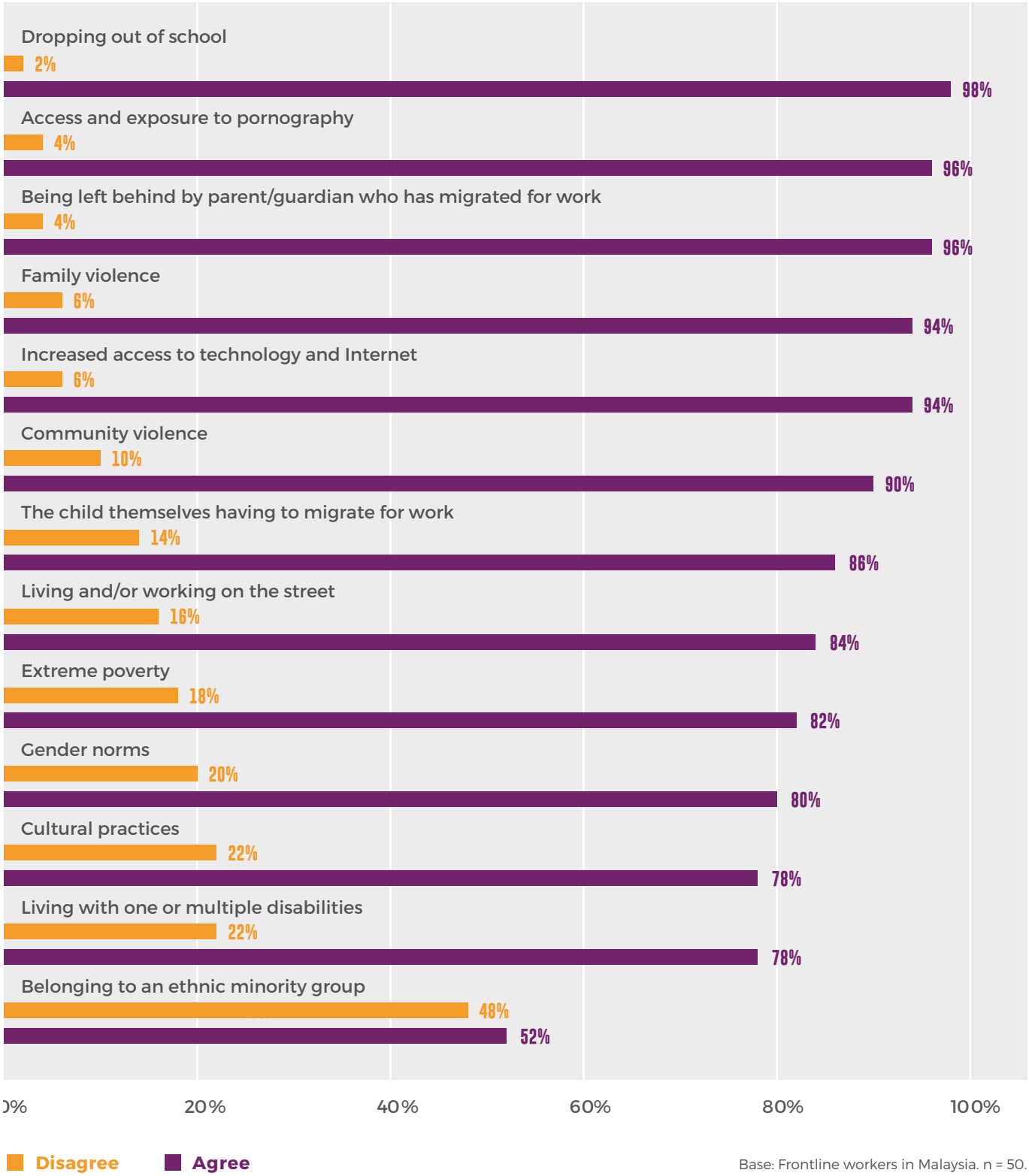
Figure 12: Caregivers' top concerns regarding their children.



Base: Caregivers of internet-using children aged 12–17in Malaysia. n = 995.

79. See for example: Crabbe, M. & Flood, M. (2021). School based Education to Address Pornography's Influence in Young People: A Proposed practice framework. *American Journal of Sexuality Education* 16(1).

Figure 13: Frontline workers' perceptions of factors related to the child that impact children's vulnerability to OCSEA.



Base: Frontline workers in Malaysia. n = 50.

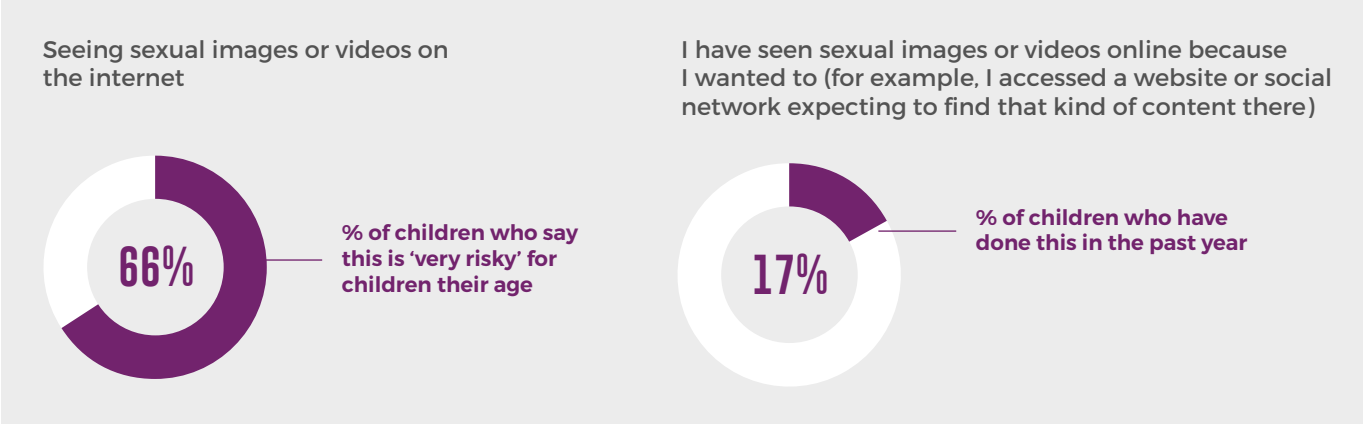
Children's experiences: Twenty-seven percent of the internet-using children reported that they had seen sexual images or videos online at least once in the past year. Seventeen percent reported actively looking for such material online and 24% had been exposed to sexual images or videos when they did not expect it. These numbers are lower than in other *Disrupting Harm* countries and may indicate a level of under-reporting, possibly because of general discomfort related to discussing this sensitive topic or because possessing and circulating pornography is criminalised in Malaysia.[80]

In conversations with four survivors of OCSEA from Malaysia conducted for *Disrupting Harm*, three indicated that exposure to pornography was part of their experience. One young person described how she had started to access pornography on her mobile phone: *"After my mother died, I lived with my aunty and uncle. When I first lived with them, they allowed me to use the phone. I became addicted... At first it was just browsing YouTube, k-pop and there was a stage when I was browsing YouTube. There were clickable ads that kept popping out so from then on, I became addicted to watching porn. I began to watch constantly until there came a time when my family found out and confiscated the phone, so I was left without a phone for about three years."* (RA5-MY-02)

Older children aged 16–17 and boys were somewhat more likely to view sexual content online, both intentionally and accidentally. For example, 27% of boys said they had come across sexual content online by accident, 70% said they had not and 3% said they did not know or preferred not to answer the question. Among girls, these percentages were 19%, 78% and 4%, respectively.

Fifty-seven percent of the children who had seen sexual images or videos online involuntarily said they had seen them in advertisements (e.g., pop-ups). Thirty-four percent had come across sexual content via social media feeds and 29% while using search engines or via direct messaging apps. Among the boys who had seen sexual content by accident, 62% had come across it in advertisements, as compared to 51% of the girls, whereas 35% of the girls had been sent the images via direct messaging as compared to 25% of the boys. The proportion of children exposed to such content who had received it via direct messages was higher among younger children (12–13: 40%; 16–17: 19%).

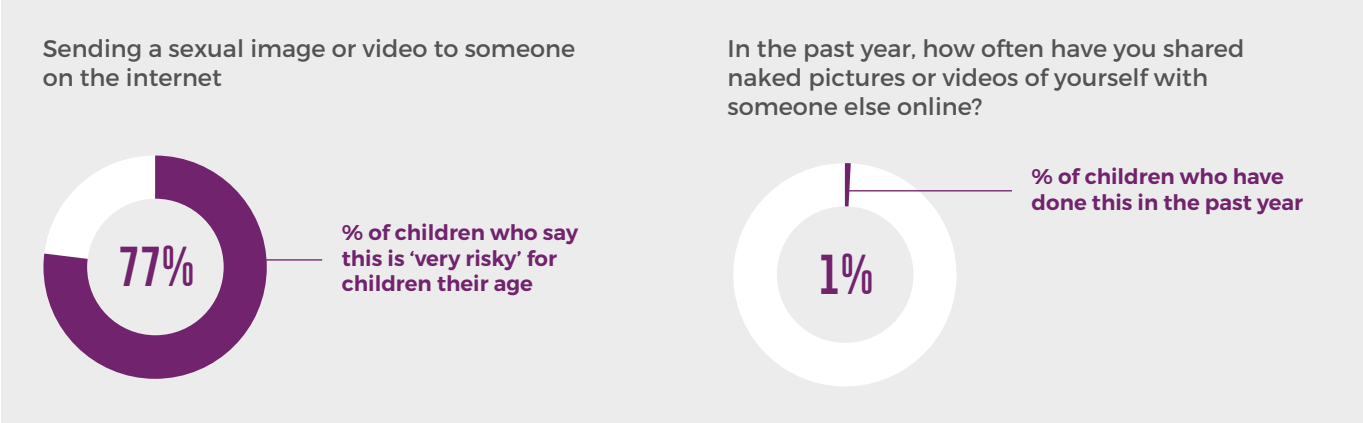
Figure 14: Children's risk assessment of seeing sexual images or videos online versus children who have actively looked for this content in the past year.



Base: Internet-using children aged 12–17 in Malaysia. n = 995 children.

80. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Section 292.

Figure 15: Level of risk attributed by children to sharing sexual content online.



Base: Internet-using children aged 12–17 in Malaysia. n = 995 children.

1.3.3 Making and sharing self-generated sexual content

Seventy-four percent of the children and 81% of the caregivers surveyed agreed with the following statement: "It is wrong for a person to take naked images or videos of themselves".

Sharing sexual images or videos was the online activity that was most commonly perceived as 'very risky' by both the children and the caregivers surveyed. Sending a sexual image or video to someone online was considered 'very risky' by as many as 77% of children and 87% of caregivers. In practice, only 1% of the children in the household survey (six children) said they had shared naked pictures or videos of themselves online in the past year. Again, these figures could be under-reported due to the common discomfort around openly discussing sex or for fear of potential criminal self-incrimination.

Meanwhile, 1% of children said they had allowed another person to take naked pictures or videos of them.

When asked to select one or more reasons why they had shared naked images or videos of themselves, two of the six children said that they were flirting or having fun and one that they were in love. These are also the most common reasons cited by children in *Disrupting Harm* countries in which sharing naked images or videos was more common.

Of the six children, one had shared the images or videos with a romantic partner and two with someone they first met online who was a contact of a friend or of a family member. Three children said that they did not know who they had shared the content with or preferred not to say – perhaps because they felt uncomfortable discussing the topic.

Figure 16: Reasons given by children for sharing naked images or videos of themselves.

Base: Children who have shared naked images or videos of themselves in the past year. n = 6.

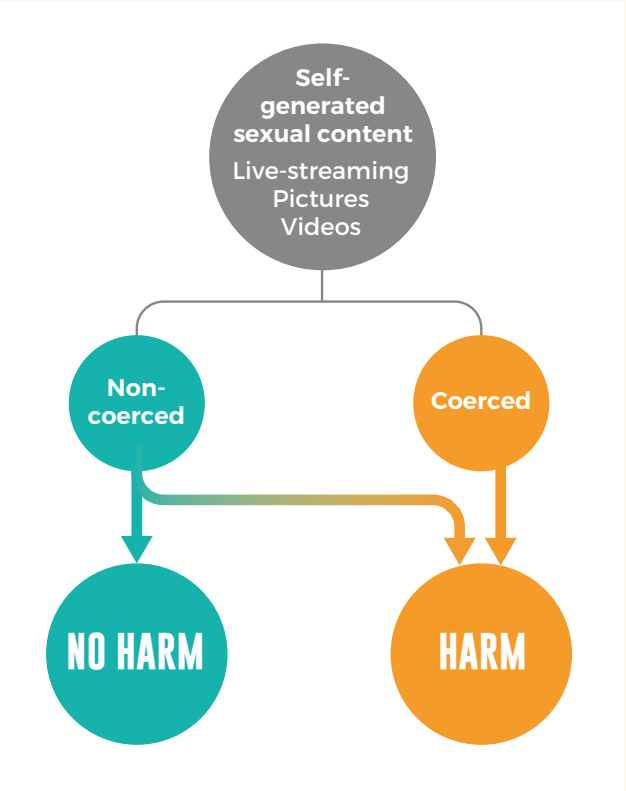
The Rise in Self-Generated Sexual Content Involving Young People

The increasing use of technology is leading to shifts in notions of privacy and sexuality among children in certain parts of the world, particularly adolescents.[81] Forms of behaviour that are increasingly normal to young people can be bewildering for adults who grew up in a different time. For instance, video live-streaming is common, whether among small private groups of friends or anonymous public audiences. While much of the live-streaming is harmless, there is an increase in producing and sharing self-generated sexual content, which can bring significant risks.[82]

The sharing of self-generated sexual content by children is complex and includes a range of different experiences, risks and harms. As the *Disrupting Harm* data shows, some self-generated content is shared with others because children are in love or having fun; such exchanges are increasingly becoming part of young people's sexual experiences. However, the data also shows that the creation and sharing of self-generated sexual content can be coerced through threats or peer pressure (see chapter 2.2).

While coercion can clearly be seen as a crime and leads to harm, there can be negative consequences for children sharing any sexual content, including cases in which the sharing is not coerced. Material shared voluntarily may not cause harm at first, but there remains a risk that it will later be shared beyond the control of the person who created it. Once it exists, such content can also be obtained deceptively or through coercion and be perpetually circulated by offenders.[83,84]

Figure 17: Mapping the consequences of sharing self-generated sexual material involving young people.



In Malaysia, a substantial proportion of 12–17-year-olds (77%) seem to be aware that producing and sharing sexual content can carry risks for children. In addition, relatively few children appear to engage in this kind of behaviour. The possible risks that sharing sexual content online entails should be central to all discussions with children about their internet use – at home, at school and in the community.

81. Livingstone, S. & Mason, J. (2015). Sexual Rights and Sexual Risks among Youth Online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments. London: European NGO Alliance for Child Safety Online.
82. Thorn & Benson Strategy Group. (2020). Self-Generated Child Sexual Abuse Material: Attitudes and Experiences.
83. Bracket Foundation. (2019). Artificial Intelligence: Combating Online Sexual Abuse of Children.
84. EUROPOL. (2019). Internet Organised Crime Threat Assessment 2019. Netherlands: EUROPOL.

It can be difficult for children to seek help if sexual content involving them is shared with others without permission, partly owing to the fear of victim blaming. In Malaysia, the household survey showed that a large majority of children (78%) and caregivers (83%) believe that, should a self-generated image or video be shared further, it is the victim's fault. When self-generated content is shared without permission, reluctance or an inability to seek help may lead to further harm for children.

Finally, victims who are coerced or manipulated into sharing sexual content may be reluctant to report as they could expose themselves to criminalisation under the generalised ban on pornography or under the provisions on sharing CSAM, as no exemption from criminal liability for children is included in the Sexual Offences against Children Act. This is particularly relevant as the minimum age of criminal responsibility is set at 10 years old in Malaysia.[85].

1.3.4 Knowledge and skills for online safety

While 61% of the children surveyed in Malaysia felt they knew more about the internet than their caregivers, there were variations among age groups (12–13: 48%; 16–17: 74%) and between children living in urban areas (64%) and those living in rural areas (55%).

Thirty-seven percent of the internet-using children who took part in the household survey in Malaysia (41% of girls and 34% of boys) said they had received information about how to stay safe online. However, 44% said that they had never received such information. The remainder said they did not know or did not answer the question – perhaps suggesting that they had no idea what such information might look like.

When questioned about their skills for staying safe online, the children surveyed seemed to be more confident in their ability to judge situations than in their operational skills. A majority expressed confidence in their ability to judge which images of themselves or their friends to share online (84%) and when to remove people from their contact lists (80%). However, the proportions of children who said they knew how to change privacy settings (67%), report harmful content on social media (66%) and check whether a website can be trusted (57%) were lower. Without these digital skills, children are not as well equipped as they could be to stay safe online.

Younger children aged 12–13 were less likely to know how to use security features than older children aged 16–17, and children in rural areas appeared to be less digitally skilled than those living in urban areas. For example, only 43% of children in rural areas knew how to check if a website can be trusted as compared to 63% of children in urban areas. Similarly, fewer children in rural areas would know how to report harmful content on social media (rural: 58%; urban: 70%). No differences were observed according to gender.

85. Nevertheless, a person above 10 years old and under 12 years' old who has not attained sufficient maturity of understanding to judge the nature and consequence of their conduct is not liable for any offence. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Sections 82 and 83.

2. ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN MALAYSIA

Following on from children's perceptions of, and participation in, various risky online practices, this chapter turns to the threat of online child sexual exploitation and abuse (OCSEA) in Malaysia. The chapter draws on a variety of sources – including law enforcement data, mandated reports from U.S.-based technology companies to the National Center for Missing and Exploited Children (NCMEC) related to Malaysia, surveys with frontline workers and conversations with children themselves and the household survey – in order to create a well-rounded presentation of the nature of these crimes against children. Chapter 2.1 is mainly concerned with law enforcement data, and chapters 2.2 and 2.3 are based largely on children's self-reported experiences.

The various indicators related to the occurrence of OCSEA contained in this chapter are not intended to provide a conclusive picture of its prevalence. There are several reasons for this. Firstly, the existing administrative data accessed, such as that kept by law enforcement authorities, rarely delineates or classifies OCSEA elements. Secondly, with respect to the household survey, one would expect a degree of under-reporting due to privacy concerns, hesitation to discuss sex and sexuality, fear of stigma and possible fear of criminal liability (related in part to the age of consent, the age of criminal liability, the criminalisation of male homosexuality and the ban on pornography). Furthermore, in households in which sexual abuse occurs, it is less likely that permission would be given for children to be interviewed for such a survey.

The survey only included internet users and children who live at home and may not, therefore, represent vulnerable populations such as children engaged in or affected by migration, street-connected children or children living in institutions. Finally, many estimates are based on the analysis of sub-samples of the survey data, which are small because OCSEA is still a rarely reported phenomenon, resulting in a larger margin of error.

While *Disrupting Harm* has full confidence in the data and the quality of the sample obtained, the challenges involved in researching specific and sensitive phenomena lead to the loss of some precision in the final estimate. For these reasons, it is suggested that the reader interprets the findings in this chapter as *a good approximation* of the occurrence of certain crimes against children related to OCSEA in Malaysia and the extent to which internet-using children in Malaysia are subjected to OCSEA.

2.1 LAW ENFORCEMENT DATA

The analysis in this chapter draws on qualitative and quantitative data from law enforcement authorities and several partner organisations, with a view to understanding the relevant offences, offender and victim behaviours, crime enablers and vulnerabilities.

2.1.1 Reported CSEA and OCSEA offences

Number of offences

The D11 division (Sexual, Women and Child Investigation) of the Royal Malaysia Police is the specialised unit responsible for combating online crimes and domestic violence, including any technology-related crime. The division provided the following information concerning the cases of sexual exploitation and abuse against children that it recorded in 2017–2019. These are the recorded numbers of cases by the specialised unit and in no way give the complete picture of the prevalence of OCSEA in Malaysia.

The D11 division identifies and disaggregates crime data for OCSEA-related crimes, which was not the case in all target countries. As the figure shows, there were many more cases recorded as CSEA than OCSEA. However, it is likely that some of the offences classed as CSEA, including those related to the sale of prohibited images, may have also contained an online or technological element, but were not recorded as OCSEA-related crimes.

Types of offence

According to law enforcement officials, the OCSEA cases investigated included grooming, abuse in person and the sharing of images on social media. Social media platforms were used to communicate, to share images and even to sell new-born children.

Figure 18: Recorded CSEA and OCSEA cases, 2017–2019.

		2017	2018	2019
CSEA	Rape	1257	1028	1191
	Sexual offences against children (Sexual Offences against Children Act, Sections 14 and 15)	271	631	752
	Incest	253	227	258
	Unnatural sexual acts	234	117	135
	Sale, etc, of prohibited images of children (Penal Code, Section 292)	6	2	0
OCSEA	Grooming (Sexual Offences against Children Act, Sections 11–13)	4	3	9
	Offences relating to child grooming (Sexual Offences against Children Act, Section 5–10)	6	7	6

Base: D11, Division of the Royal Malaysia Police.

Most of the offences were committed offline with the use of a smart phone or mobile device to record. The children were solicited directly by the offenders, with the exception of one case in which a facilitator was identified. The number of charges for the possession of child sexual abuse material (CSAM) was relatively high, while the number of charges for CSAM production was lower.

In a majority of the cases, sexual gratification was identified as the primary motivation for offenders. Monetary gain was the driving factor in one case only. In that particular case, the mother of the victim and her boyfriend coerced her to engage in sexual intercourse with two other men in exchange for cash, which was kept by the mother.

According to one government interviewee: *"Child sexual abuse materials, grooming and sexual extortion are the most common offences under OCSEA categories in Malaysia".* The interviewee also highlighted that there were currently no registered cases related to the live-streaming of child sexual abuse in Malaysia. (RA1-MY-11-A)

Offenders

According to the law enforcement interviews, all the offenders in the OCSEA cases handled by the D11 division were persons in close proximity to the victims. Only in one case was there a link to the travel and tourism industry.

The data on these cases shows that offenders were overwhelmingly men. In the year 2017, seven cases were recorded against male offenders and one against a female offender. In 2018, a total of eight cases were recorded against male offenders, while in 2019, a total of twelve cases were recorded against male offenders and one case against a female offender.[86]

Figure 19: Age group of offenders.

Offender in age brackets	2017	2018	2019
Under 18	3	1	0
18–29	1	2	5
30–39	3	3	1

Base: D11, Division of the Royal Malaysia Police.

Victims

In the cases investigated by the D11 division, the victims were most commonly girls aged 13 to 15.

Figure 20: Age group of victims.

Victim age bracket	2017	2018	2019
4–6	0	1	0
7–9	0	3	1
10–12	0	0	2
13–15	4	4	6
From 16 but under 18 years old	2	0	5

Base: D11, Division of the Royal Malaysia Police.

Figure 21: Gender of victims.

Gender	2017	2018	2019
Male	1	1	2
Female	5	7	12

Base: D11, Division of the Royal Malaysia Police.

In all the cases investigated by the D11 division, the victims were Malaysian nationals and were living at home with family members. In the *Disrupting Harm* survey of frontline workers in Malaysia, 84% agreed that "living or working on the streets" was a factor that contributed to a child's vulnerability to OCSEA. As many as 96% agreed that parents migrating for work and leaving children behind contributed to a child's vulnerability, yet this data shows that OCSEA can affect all children, even those without obvious vulnerabilities. Moreover, this may also indicate that cases involving children not living with family members go unreported.

The law enforcement data for Malaysia revealed that frequently, when cases of OCSEA involved multiple victims, the children were often friends or children of similar ages with a connection through school, the community or the neighbourhood.

86. Allnock D, Atkinson R. 'Snitches get stitches': School-specific barriers to victim disclosure and peer reporting of sexual harm committed by young people in school contexts. Child Abuse Negl. 2019 Mar;89:7-17. doi: 10.1016/j.chiabu.2018.12.025. Epub 2019 Jan 3. PMID: 30612073.

Figure 22: CyberTips concerning suspected child sexual exploitation in Malaysia.

	2017	2018	2019	% Change 2017 to 2019	% Change 2018 to 2019
Malaysia	96,627	219,459	183,407	90%	-16%
Global total	10,214,753	18,462,424	16,987,361	66%	-8%
Malaysia % of Global total	0.95%	1.19%	1.08%		

Base: CyberTip data provided by NCMEC.

Enablers

According to the law enforcement officials interviewed for *Disrupting Harm*, children in the cases investigated by the Malaysian police were approached and groomed by offenders offline. All victims in these cases were abused by either a parent or an adult guardian. The physical proximity of the offender to the victim and their position of power further exacerbated the situation. Coercion, threats and persuasion were employed in different ways in the cases, sometimes with goods and money being exchanged. Money was reported to have been exchanged in some cases involving girls. In another case in which the offender was a teacher, it was reported that the offender bought clothes, shoes and mobile phones for the victims (in this case boys) in exchange for the abuse. After the abuse occurred, images and videos were commonly shared. Police indicated that no sophisticated methods were employed. Online social media platforms were used to share images.

The law enforcement authorities perceived the increase in OCSEA-related crime rates to be largely attributable to the widespread use of mobile devices, inexpensive and high-speed internet connections, the lack of safe spaces for dialogue on sexual offences and a low number of convictions. In the qualitative interviews concerning the country capacity, the law enforcement authorities recognised the impact of each of these factors independently and collectively, and demonstrated the will and preparedness to upskill themselves, allocate resources and engage with the technology industry to enhance coordination and cooperation.

2.1.2 International OCSEA detections and referrals

Trends in CyberTips

On behalf of the Malaysian law enforcement authorities, data was requested for *Disrupting Harm* from the U.S. National Center for Missing and Exploited Children (NCMEC) related to CyberTips concerning suspected child sexual exploitation in Malaysia for the years 2017 to 2019.

United States federal law requires 'electronic service providers' (i.e., technology companies) based in the United States to report instances of suspected child exploitation on their platforms to NCMEC's CyberTipline. NCMEC triages these reports and passes the CyberTips onto the national law enforcement units of the relevant countries for action. However, for providers not based in the United States, this reporting is voluntary. As not all platforms notify suspected child exploitation to NCMEC, the data below does not encompass a number of platforms popular in the *Disrupting Harm* focus countries.

After a year-on-year increase of 127% in 2018, reports for Malaysia declined by 16% in 2019. This represents an overall increase of 90% from 2017 to 2019 in Malaysia.

Types of OCSEA offences

The possession, manufacture and distribution of CSAM (referred to in U.S. legislation as 'child pornography') accounted for almost all of the NCMEC CyberTips for Malaysia between 2017 and 2019.

Figure 23: CyberTips concerning suspected child sexual exploitation in Malaysia, by incident type.

Incident Type	2017	2018	2019
CSAM, including possession, manufacture and distribution (NCMEC classification: child pornography)[87,88]	96,594	219,433	183,383
Travelling child sex offences (NCMEC classification: child sex tourism)[89]	1		
Child sex trafficking	2	1	1
Child sexual molestation		1	5
Misleading domain name	1		
Misleading words or digital images on the internet		5	2
Online enticement of children for sexual acts	28	17	14
Unsolicited obscene material sent to a child	1	2	2
Malaysia Total	96,627	219,459	183,407

Base: CyberTip data provided by NCMEC.

Reports relating to CSAM increased by 90% between 2017 and 2019. While the numbers of other incident types were comparatively small and did not increase to such an extent, the multiple reports concerning suspected offline child exploitation may reflect Malaysia's status as a tourist destination of interest to travelling sex offenders. In fact, NCMEC's additional internal classification (Incident Type 2[90]) flagged 21 of the reports for 2017–2019 for online enticement of children pre-travel. A further 17 reports were tagged as relating to online enticement using blackmail. It is unclear from the data whether these reports concern suspects in Malaysia or victims in Malaysia, or both. In 2017–2019, two reports were classed as Priority 1, indicating a child in imminent danger.

Almost 100% of NCMEC CyberTips for Malaysia in the period from 2017 to 2019 came from electronic service providers. A total of 61 electronic service providers submitted at least one report of suspected child sexual exploitation for Malaysia in the reporting period. This would indicate some diversity in the platforms used by the general population, and by OCSEA offenders. The data for the 20 platforms that submitted the largest numbers of reports in 2019 is depicted in Figure 24.

Facebook submitted 95% of the NCMEC CyberTips for Malaysia. There was an 87% increase in the number of cases reported by Facebook in Malaysia between 2017 and 2019. There were also significant increases in the numbers of cases reported by Google (86%), Instagram (395%) and WhatsApp (368%) between 2017 and 2019. The number of cases reported by Twitter declined slightly.

87. The terminology used in this column reflects the classification by the National Center for Missing and Exploited Children in line with U.S. legislation. *Disrupting Harm* advocates the use of the term 'child sexual abuse material', in line with the Luxembourg Guidelines.
88. CyberTips under this category may reference more than one file of CSAM. For example, some reporting electronic service providers include more files per report, as opposed to one image per report and multiple reports per suspect.
89. The terminology used in this column reflects the classification by the National Center for Missing and Exploited Children in line with U.S. legislation. *Disrupting Harm* advocates use of the term 'travelling child sex offences', in line with the Luxembourg Guidelines.
90. Incident Type 2 (IT2) is an additional classification by NCMEC, including additional disaggregated data. IT2 classifications may include auto-referred international, unconfirmed files (files not reviewed by NCMEC), online enticement blackmail, child images (clothed), not enough information (dummy record), animation drawing or virtual, images appearing adult. IT2 does not indicate imminent threat and is not necessarily associated with Priority levels.

Figure 24: CyberTips concerning suspected child sexual exploitation in Malaysia, by reporting electronic service providers.

Reporting Electronic Service Provider	2017	2018	2019
Facebook	92,138	211,739	172,294
Instagram Inc.	1,341	4,077	6,637
Google	1,636	2,469	3,045
Twitter Inc./Vine. co	376	324	335
WhatsApp Inc	50	160	234
Tumblr	204	268	227
MeWe			109
Imgur LLC	14	4	92
Tagged.com	38	42	83
Pinterest Inc	63	76	68
Microsoft – Online Operations	24	34	38
Snapchat	3	19	38
Discord Inc.	1		36
Dropbox Inc.	21	9	23
MeetMe.com (fkamyYearbook.com)	41	17	16
Yahoo!Inc	57	37	15
SmugMug-Flickr		13	13
Stelivo LLC			9
Omegle.com LLC	9	8	7
Younow.com	7	1	7

Base: CyberTip data provided by NCMEC, sorted by 2019 counts, null results removed.

> The OCSEA cases investigated by the specialised unit included grooming, abuse in person and the sharing of images on social media.

Figure 25: CyberTips concerning suspected child sexual exploitation in Malaysia – number of unique upload IP addresses by year.[91]

	2017	2018	2019	% Change 2017–2019	% Change 2018–2019
Malaysia Unique Upload IP Addresses	56,896	95,367	102,861	81%	8%
Total Malaysia Reports	96,627	219,459	183,407	90%	–16%
Reports per Unique IP Address	1.70	2.30	1.78	5%	–23%

Base: CyberTip data provided by NCMEC. NB: The same IP address may be counted in more than one year.

A very wide range of social platforms and image hosting and video sharing providers, including randomised video chat companies, reported cases for Malaysia. Of note, privacy-focused social media platform MeWe made 109 reports in 2019 related to Malaysia. The presence in the data of self-avowed "moral free file host" Motherless.com, anonymous image-based bulletin board 4chan, anonymous social media app Whisper, virtual private server host Stelivo, digital forensics research company Hacker Factor, and dark web and peer-to-peer monitoring firm Tiversa (346 reports in 2017) may also indicate the presence of OCSEA offenders in Malaysia with a level of technical sophistication and specialist interest. Reports from platforms Discord (36 reports in 2019) and Twitch, often used to facilitate gaming chat and streaming, may reflect Malaysia's adoption of tools and apps requiring greater bandwidth.

The variety of platforms among the reporting Electronic Service Providers may also provide information regarding the nature of suspected OCSEA offending. Multiple reports from Tagged.com (163 in total) and Skout.com (38 in total), and the appearance of Match, Tinder, OkCupid and Initech/Growlr, point to the misuse of over-18 dating sites for suspected distribution of CSAM. Moreover, the appearance of Chaturbate, a platform specialising in the provision of adult live-streamed sexual activity that is often paid for in tokens, and payments provider PayPal, may indicate the use of OCSEA for commercial purposes.

Number of IP addresses reported

NCMEC CyberTips also permit the analysis of headline statistics for unique internet protocol (IP) addresses used to engage in suspected child exploitation (see Figure 25).

An IP address is assigned to each individual device on a specific network at a specific time. The number of unique IPs routed through Malaysia increased in each year of the reporting period, despite the fall in NCMEC CyberTips in 2019, while the average number of reports per unique IP address peaked in 2018. A higher report rate per unique IP address is suggestive of a tendency for offenders (or at least their devices) to upload multiple items of CSAM in a detected session, thereby generating multiple reports with the same upload IP address.

Furthermore, a report may contain more than one upload IP address. This would perhaps reflect more than one instance of suspected child sexual exploitation, as would be the case for manual reports that collate multiple events for a single suspect. They may also reflect a dynamic assignment of IP addresses by the suspect's telecommunications provider. For instance, if a suspect's internet connection is refreshed while uploading CSAM to a particular platform, it is possible that more than one IP address is assigned to that device by the telecommunications provider and, therefore, captured by the platform reporting to NCMEC.

91. Note: The same IP address may be counted in more than one year, and a report can contain more than one unique IP address. Technical measures by ISPs including the dynamic assignment of IP addresses and the sharing of IP version 4 addresses across a large number of devices can also have an impact on the number of unique IP addresses logged.

The ongoing transition from version 4 of the Internet Protocol address system (IPv4), which in recent years has shared 32-bit IP addresses among a large number of devices by means of carrier grade Network Address Translation, to version 6, which assigns unique 128-bit addresses for devices, may also have a bearing here. Scrutiny of the content of NCMEC CyberTips received by Malaysia would be required to test these hypotheses.

2.1.3 Evidence of CSAM from other sources

CSAM distribution on peer-to-peer networks

Although CSAM is usually shared via social media, traditional peer-to-peer sharing persists. Data from the Child Rescue Coalition, which detects the distribution of CSAM on peer-to-peer file-sharing networks, concerning peer-to-peer distribution of CSAM between 9 June 2019 and 8 June 2020 is given in Figure 26. Since the system does not monitor all file-sharing networks, this figure should be treated with caution. The high number of Global Unique Identifiers[92] as compared to IP addresses in Malaysia may indicate that offenders delete the software frequently and reinstall it when they want to share material.

Figure 26: CSAM distribution and downloading of CSAM on file-sharing networks in the Disrupting Harm focus countries in Southeast Asia.

	IP Addresses	Globally Unique Identifiers GUIDs
Cambodia	1319	95
Indonesia	1124	202
Malaysia	**2754**	**558**
The Philippines	1971	1446
Thailand	3049	609
Vietnam	925	141

Base: Data supplied by the Child Rescue Coalition for the period from 9 June 2019 to 8 June 2020.

During the reporting period, offenders in Malaysia displayed a tendency to delete their software after each use, or from time to time, and to reinstall it when they wanted to share and download again. In other words, the high discrepancy between the number of addresses and the number of globally unique identifiers may indicate the use of dynamic IPs by offenders to exchange CSAM.

Distribution on peer-to-peer networks is less of an 'entry level' activity than distribution on mainstream social media platforms, since users are required to download specialist software and to actively upload and search for CSAM, which is often done by file names shared in offender networks. The capture of multiple IP addresses per installation of file-sharing software (represented by the number of Globally Unique Identifiers in the above figure) indicates that the average Malaysian offender engaged in multiple sessions of CSAM distribution in the period studied.

CSAM distribution via Twitter

Twitter has analysed about three million URLs shared by accounts suspended for the violation of the platform's CSEA policy. This analysis, conducted by Twitter on behalf of *Disrupting Harm*, confirmed that in 2017–2019, a number of users in Malaysia were suspended for suspected CSEA-related activity. The email addresses linked to these accounts were predominantly generic web-based accounts such as Gmail, Hotmail/Outlook and Yahoo Mail. In terms of the behaviour of these suspended profiles, there was a desire to move onto more private channels such as direct messaging, or more private platforms. Activity on private channels related to live-streaming indicated Skype as the dominant platform.

Web Searches for CSAM

Research was conducted on Google Trends to find out how often searches were conducted by Google users in Malaysia using search terms likely to be used to reach CSAM on the internet. In the first instance, a sample of 20 terms selected by INTERPOL served as keywords and phrases for specialist interest in CSAM. Queries for the time period 1 January 2017 to 31 December 2019 on searches in Malaysia returned a result of 'not enough data' for each of these 20 terms.

92. A Globally Unique Identifier (GUID) is a 128-bit number created by the Windows operating system or another Windows application to uniquely identify specific components, hardware, software, files, user accounts, database entries and other items.

Although individuals in Malaysia looking for CSAM may search in languages other than English, there is no information on the use of search terms in local languages or slang. The law enforcement authorities could fill this gap by reviewing OCSEA investigations in Malaysia with a view to identifying additional terms and search strings used by offenders. The results cited above, nevertheless, appear to demonstrate that there is an appetite for CSAM in Malaysia, and that the open web is used to discover it.

CSAM hosting

Malaysia has been identified as a hosting country for images and videos assessed as illegal by INHOPE member hotlines contributing to the ICCAM platform,[93] as follows:

Figure 27: CSAM hosting in Malaysia, as identified by INHOPE member hotlines using ICCAM.

Year	Illegal Items	Percentage of Global Total
2017	12	0.01%
2018	16	0.01%
2019	608	0.19%

Base: Data provided by INHOPE.

While the percentage of global hosting remains small, the number of illegal items identified as hosted in Malaysia increased in 2019. To some extent, this can be explained by operational considerations, including increased identification of CSAM worldwide following the deployment of the Project Arachnid web crawler in 2018.[94] The Internet Watch Foundation, meanwhile, actioned the following reports concerning confirmed CSAM hosting in Malaysia:

Figure 28: CSAM hosting in Malaysia, as identified by the Internet Watch Foundation.

Year	Illegal Items	Percentage of Global Total
2017	7	0.01%
2018	12	0.01%
2019	55	0.04%

Base: Data provided by Internet Watch Foundation.

2.1.4 Links to travel and tourism

The Angel Watch Center of U.S. Homeland Security Investigations provides referrals to officials in destination countries on convicted U.S. child sex offenders who have confirmed scheduled travel. In 2017, five referrals were made to Malaysia and three were denied entry to the country. The following year saw eight referrals, and no one was denied entry. In 2019, there were eight referrals and three were denied entry. Confirmed entry denials indicate positive coordination between Malaysia's Bureau of Immigration and Human Trafficking (D3), the Organised Crime Investigation Unit (D14) and the Sexual, Women and Children Investigation Division (D11) Unit of the Royal Malaysia Police.

Officials of law enforcement agencies from countries other than the United States also informed *Disrupting Harm*, on condition of anonymity, that they were aware of sex offenders travelling to Malaysia. One agency confirmed that one known child sex offender travelled to Kuala Lumpur in 2019. The national child sex offender registry in another country indicates that 18 child sex offenders are suspected to have undertaken travel to Malaysia between January 2015 and May 2020. A third foreign law enforcement agency reported that they had data of 20 suspected cases of online child sexual exploitation in Malaysia in 2017, 29 in 2018 and 87 in 2019.

93. INHOPE. (n,d). What is ICCAM & Why is it important?
94. Operated by the Canadian Centre, Project Arachnid is an innovative tool designed to crawl links on sites previously reported to Cybertip.ca that contained CSAM and detect where these images/videos are being made publicly available. Once child sexual abuse material is detected, a notice is sent to the provider hosting the content requesting its removal.

2.2 CHILDREN'S EXPERIENCES OF ONLINE SEXUAL EXPLOITATION AND ABUSE IN MALAYSIA

Under the *Disrupting Harm* project, OCSEA is specifically defined to include online grooming of children for sexual purposes, the production, possession or sharing of CSAM and the live-streaming of child sexual abuse. These concepts are used in this chapter to organise and present the results of the *Disrupting Harm* research. Moreover, we recognise that the ways in which children are subjected to OCSEA are far more complex and nuanced. The experiences or offences in question often occur in combination or in sequence. Furthermore, as explored in the box on *The Continuum of Online and Offline Child Sexual Exploitation and Abuse* on page 68, OCSEA only sometimes occurs exclusively in the digital environment, but frequently digital technology is used as a tool to facilitate or record in-person sexual exploitation and abuse.

Relatively few children said they were subjected to OCSEA, potential grooming and other unwanted experiences online. Therefore, many of the follow-up questions involve small sub-samples. In such cases, when the sample is smaller than 50, absolute numbers are presented instead of percentages to avoid mis-representation of the data.

Recognising that sexual exploitation and abuse of children can happen in many different ways and places, most of the survey questions referred to below allowed for multiple responses, so the proportions and figures presented may not add to 100%. Finally, differences between age groups, boys and girls, or urban and rural areas are only reported when they are five percentage points or more.

An Overview of the Survey Data on Instances of OCSEA

In the *Disrupting Harm* household survey, children were asked whether they had experienced different potential or actual forms of online sexual exploitation and abuse. For this analysis, we include only the following clear examples of online sexual exploitation and abuse.

Children were asked if ***in the past year***, they had experienced any of the following:

1. Someone offered you money or gifts in return for sexual images or videos.
2. Someone offered you money or gifts online to meet them in person to do something sexual.
3. Someone shared sexual images of you without your consent.
4. Someone threatened or blackmailed you online to engage in sexual activities.

When taken together, the data reveal that, in the previous year alone, an estimated 4% of internet-using children aged 12–17 in Malaysia (38 children) had been subjected to clear instances of online sexual exploitation and abuse: a relatively low figure in comparison to other Southeast Asian countries in which *Disrupting Harm* was conducted. [95]

Nevertheless, when scaled to the population of internet-using children in this age group, the findings suggest that an estimated 100,000 children in Malaysia may have been subjected to at least one of these harms in a single year. Moreover, OCSEA may have been under-reported in the household survey for the reasons explained at the beginning of this chapter (e.g., shame or discomfort talking about sex, fear of stigma or fear of criminal self-incrimination) (see page 44).

95. The Philippines (20%); Cambodia (11%); Thailand (9%); Indonesia (2%); Vietnam (1%).

Children offered money or gifts for sexual images or videos

The offer of money or gifts to a child in return for sexual images or videos constitutes evidence of grooming with the aim of obtaining CSAM. Among the internet-using children surveyed, 2% (17 children) said that someone had offered them money or gifts in return for sexual images or videos within the past year.

What is Online Grooming?

Disrupting Harm defines online grooming as engaging a child via technology with the intent of sexually abusing or exploiting the child. This may happen either completely online or via a combination of online and in-person contact.

Online grooming is a complex process, which is often fluid and difficult to detect, especially where it involves a slow building of trust between the offender and the child over an extended period of time. The child is often 'prepared' for sexual abuse and made to engage in sexual acts online or in person by means of deceit, coercion or threats. However, online grooming can also be or appear abrupt, with an offender suddenly requesting or pressuring a child to share sexual content of themselves or to engage in sexual acts, including via extortion.

In Malaysia, the Sexual Offences against Children Act criminalises the act of sexually communicating with a child or encouraging a child to sexually communicate by any means.[96] This legislation could be used to address grooming in the online context (see Overview of Legislation and Policy).

Internet-using children aged 12–17 in Malaysia from the Disrupting Harm study, n = 995.

Children offered money or gifts for sexual acts

It is clear from the conversations with survivors of OCSEA conducted as part of the research for *Disrupting Harm* that grooming children online for the purpose of meeting in person to engage in sexual activities is a real threat. NCMEC CyberTips concerning suspected child sexual exploitation in Malaysia presented in chapter 2.1.2 show that there were 59 reports related to online enticement of children for sexual acts in 2017–2019.

In the household survey in Malaysia, 1% of the children surveyed said that, within the past year, someone had offered them money or gifts to meet in person to do something sexual (13 children). Similar to other findings, these numbers may be under-reported as children may not feel comfortable or sufficiently safe to disclose their experiences of abuse and exploitation.

Base: Internet-using children aged 12–17 in Malaysia from the Disrupting Harm study, n = 995.

96. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section. 11.

Sexual extortion

Sexual extortion is sometimes used in the grooming process. Offenders may have already obtained sexual images or videos of children through deceit or coercion and can threaten to make those images publicly available or share them with the child's friends or members of their families, as a way of pressuring children into sharing more images or engaging in sexual activities. Such threats can also be used to extort money. Malaysian legislation criminalises those who threaten to use any representations of the sexual parts of a child or a child engaged in sexual activities.[97] However, this provision is not specific to the act of using such material to extract sexual content or other benefit from the child.

In the household survey, internet-using children in Malaysia were asked if anybody had "threatened or blackmailed you to engage in sexual activities" within the past year. One percent (12 children) said 'Yes'. Another 3% of children did not answer the question, which may indicate under-reporting due to sensitivity. The children were not asked what kinds of threats were used, so it is not clear, for example, whether previously obtained sexual images were used to extort money or to pressure the children to engage in further sexual activities. However, conversations with young people who were survivors of OCSEA illustrate how threats were used to extort further sexual activity: *"They said, 'Don't tell the family. If you do, I will come after you,' so I was like, 'OK, I won't tell anyone'."* (RA5-MY-03)

Base: Internet-using children aged 12–17 in Malaysia from the Disrupting Harm study. n = 995

Children's experiences of non-consensual sharing of sexual images

NCMEC CyberTips presented in chapter 2.1.2 show that the possession, manufacture and distribution of CSAM accounted for the vast majority of Malaysia's NCMEC CyberTips in 2017–2019.

Of the internet-using children aged 12–17 in Malaysia who took part in the *Disrupting Harm* household survey, 3% (25 children) stated that someone had shared sexual images of them without their permission.

Base: Internet-using children aged 12–17 in Malaysia from the Disrupting Harm study. n = 995.

Sexual images of children, particularly those shared online, can be circulated widely and viewed repeatedly all over the world, resulting in a continuous sense of shame and fear of being recognised for the victims. When these images or videos capture instances of severe sexual abuse, the trauma associated with those in-person experiences can also be repeatedly reactivated by the sharing of the content.

In the household survey, 79% of children and 84% of caregivers stated that sharing naked images or videos of other people should be illegal.

97. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017. 15(b).

How technological development has influenced OCSEA

The wide availability of faster and cheaper internet access has led to the increasing use of video tools in communications. Video chat and live-streaming tools have rapidly gained popularity and are changing the ways in which we engage with each other, particularly for young people. Live-streaming is increasingly used both among small private groups and for 'broadcasts' to large, public, unknown audiences. In Malaysia, 72% of internet users aged 12–17 watch live-streams at least every week.

While watching live-streams is often harmless and can have many benefits, the misuse of such tools is creating new ways of perpetrating OCSEA, including the following:

Offenders broadcasting child sexual abuse: Live-streaming tools can be used to transmit sexual abuse of children instantaneously to one or more viewers, so that they can watch it while it is taking place. Remote viewers may even be able to request and direct the abuse, and financial transactions can occur alongside it, even within the same platform.

Streaming platforms do not retain the content shared, only the metadata concerning access to their services. This means that when the streaming stops, the CSAM vanishes, unless the offender deliberately records it. This creates specific challenges for investigators, prosecutors and courts, especially as the existing legal definitions of CSAM and the methods of investigation and prosecution are not always up to date.

Self-generated sexual content involving children: As noted in chapter 1.3.3, the rise in self-generated sexual content, both coerced and non-coerced, live-streamed or recorded, poses complex challenges. Even if the production is non-coerced, this content can still make its way into circulation through sharing without permission or nefarious means such as hacking. Governments and support services everywhere are grappling with how to address these issues.

The analyses for the following sections include children who experienced any of the four clear forms of OCSEA described in the box on page 54.

Because children can be blackmailed, threatened or offered money or gifts to engage in sexual activities entirely in person (without the involvement of technology), in the subsequent analysis, only children who said that this happened online, i.e., via social media or an online game, are included as they represent cases of OCSEA.

Where and how OCSEA happens

Online or in person? Of the 38 children who had experienced at least one of the four clear forms of OCSEA in the previous year, 21 said social media was involved and seven reported that online gaming was involved. Five children reported that in-person abuse occurred as part of the OCSEA they were subjected to (for instance, some children had been offered money or gifts in person to share sexual images). Seven children preferred not to say, and another 12 children said they did not know how it occurred – understandably, children might not want to disclose the details of these experiences.

Which social media platforms? In the household survey, among the 21 children who experienced OCSEA on social media, WhatsApp, Facebook and Facebook Messenger were the platforms on which OCSEA most commonly occurred. Other known platforms (e.g., Instagram, TikTok, Snapchat, Twitter) and lesser-known platforms (e.g., Line, Periscope, Discord or live.me) were cited by fewer children. Boys and younger children aged 12–13 were more likely to be targeted through a wider range of platforms than older children aged 16–17 and girls.

Some of the children surveyed in Malaysia also reported being targeted on WeChat (three children) and Telegram (two children). As these platforms are not legally obliged to report, and do not make voluntary reports to NCMEC, it is difficult to assess the scale and scope of offences against children occurring on these platforms.

Figure 29: Social media platforms on which children experienced OCSEA in the previous year.

Social media platform	Number of children
WhatsApp	12
Facebook/Facebook Messenger	12
TikTok	4
Snapchat	4
Instagram	3
WeChat	3
Line	2
Twitter	2
Telegram	2
Periscope	1
Discord	1
Live.me	1
Tumblr	1
YouTube	1

Base: Internet-using children aged 12–17 who experienced OCSEA in the previous year in Malaysia from the *Disrupting Harm* study. n = 21.

The *Disrupting Harm* findings related to the most common platforms used in cases of OCSEA are consistent with survey data published by the Malaysian Communications and Multimedia Commission on the general popularity of online platforms. This report indicates that WhatsApp was the most popular communication app (98.1% of 27.8 million communication app users had an account), followed by Facebook Messenger (55.6%), WeChat (36.8%) and Telegram (25%).[98]

As with other spaces children inhabit, social media platforms can be misused to target children. As presented in chapter 2.1, the overwhelming majority of NCMEC CyberTips related to Malaysia were from Facebook. In the household survey, large proportions of children who had experienced OCSEA, or other suspicious and/or unwanted interactions online, also reported that the last time that this happened, it occurred on Facebook or Facebook Messenger.

Twelve children surveyed also indicated they were most recently targeted via WhatsApp – an uncommon finding in *Disrupting Harm*. Of note, both Facebook and WhatsApp are among the most popular platforms globally, which in part explains why many children experience OCSEA on these platforms. This may also indicate that offenders use Facebook as an entry point and then move victims onto other, more secure platforms such as WhatsApp. WhatsApp uses end-to-end encryption, a privacy safeguard which ensures that the images, videos, written text and live communications are visible only to the sender and recipient. While end-to-end encryption provides important privacy safeguards to children, it can be misused by offenders to conceal illicit crimes and can prevent detection and investigation of abuse by law enforcement. INTERPOL recently adopted a resolution calling on member countries to urge end-to-end encryption providers to take responsibility for designing products and services that are inherently safe for children and to ensure that they are able to respond to legal requests to provide law enforcement with relevant information.[99]

Case Study 1
Abuse Occurring on Social Media Platforms

A 25-year-old offender made contact with a 7-year-old boy via Instagram. After the initial contact, the suspect exchanged messages with the child on WhatsApp for a period of 2–3 months. The grooming by the suspect led the child to take images of his private parts and share these with the suspect. The victim was living at home with his family. The suspect also used WhatsApp video calls to communicate with the victim. When the mother of the victim checked the child's phone, she became aware of the messages between her son and the suspect. The family of the child subsequently lodged a complaint to law enforcement and provided the account details on social media and the phone number. An investigation is underway at the time of writing and involves collaboration with telecommunication companies to identify the alleged offender.

98. Malaysian Communications and Multimedia Commission (2018). Internet Users Survey 2018. Statistical Brief Number Twenty-Three.
99. INTERPOL (2021). INTERPOL General Assembly resolution calls for increased safeguards against online child sexual exploitation.

Who are the offenders?

Among the 38 children who had experienced at least one of the forms of OCSEA described above in the previous year, 10 children said that they did not know the person prior to the incident, while 18 children said they did not know who the person was.[100]

Furthermore, an important proportion of offenders in the cases of OCSEA experienced by children in the household survey were persons known to the child, particularly peers under 18 (six children), adult friends or acquaintances (five children) and family members (five children).

A similar pattern of offender profiles emerged from the *Disrupting Harm* survey of 50 frontline workers. When asked about the typical relationship of the offender to the child in the OCSEA cases they had worked on in the past 12 months, the frontline workers most commonly indicated 'strangers (nationals)', followed by 'parents/step-parents' and 'community members under 18'. The respondents indicated that facilitators[101] were not often involved.

It should be added that 11 of the 38 children who had been subjected to these clear instances of OCSEA preferred not to say who the offender was. This reluctance to disclose could indicate that the person was known to them. It may be more difficult for children to disclose when offenders are individuals they are economically and/or emotionally dependent on.

In the cases recorded by the national law enforcement authorities (see chapter 2.1), all the offenders had a close connection to the children. Parents, guardians, teachers, physical education instructors and sports trainers had used their positions of power to persuade children to produce CSAM or used their authority to abuse them. In the frontline worker survey, various respondents similarly indicated that offenders included people in positions of authority or power.

The fact that the cases recorded by law enforcement authorities all involved persons known to the child could, of course, be due to the difficulty involved in identifying anonymous internet users. Nevertheless, despite the limited evidence, there are indications that this is a common profile of offenders in Malaysia. In fact, research on sexual abuse and exploitation generally shows that offenders are often from a child's circle of trust.[102,103] Therefore, education and awareness-raising efforts should not focus disproportionately on 'stranger danger'.

Case Study 2
An Offender Misuses Position of Power

In 2019, a male school warden aged 28 was identified by police. He had groomed five children aged between 9 and 15 attending the school by showing pornographic videos. The children were assaulted on the school site. The case was reported to the police by one of the victims and the offender was investigated and charged under Section 377B and 377C of the Penal Code[104] (using provisions related to "acts against the order of nature" or homosexuality), Sections 15 (e) and 16 (1) of the Sexual Offences against Children Act 2017[105] and Section 5 (1) (a) of the Film Censorship act of 2002.[106] The suspect was sentenced to 133 years in jail and 42 rattan strokes.

100. Survey responses included "Someone I did not know prior to the incident" (i.e., the identity of the offender is now known to children, yet the individual was unknown to the child until the incident occurred) and "I don't know who the offender is" (i.e., someone whose identity they still do not know after the incident occurred. Nevertheless, the offender could be someone the child actually knows or someone unknown).
101. 'Facilitator' was explicitly defined for the survey participants to answer this question as: "individuals or entities whose conduct (behaviour) facilitates or aids and abets the commission of a sexual offence against the child (sometimes referred to as 'intermediaries')".
102. Finkelhor, D. (2012). Characteristics of crimes against juveniles. Durham, NH: Crimes against Children Research Center.
103. Whealin, J. (2007). "Child Sexual Abuse". National Center for Post-Traumatic Stress Disorder: U.S. Department of Veterans Affairs.
104. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017, Section 292.
105. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017.
106. Government of Malaysia (2002). Film Censorship Act.

Disclosing OCSEA

Ten of the 38 children who had experienced one or more of the above forms of OCSEA in the previous year did not tell anyone what had happened (as an exception, all of the children who had been offered money or gifts in exchange for sexual acts did tell someone the last time this happened). Children who disclosed were most likely to confide in a friend (18 children) or a sibling (11 children). A proportion of children turned to a male caregiver (seven children) or a female caregiver (four children) – particularly in the case of younger children and girls. In a smaller number of cases, the children turned to a teacher (four children) or another trusted adult (one child).

None of the children who had experienced the clear forms of OCSEA reported to the police or to a social worker. Only one girl, who was offered money or gifts for sexual images, called a helpline. This is in accordance with earlier research findings that indicate that children are not likely to turn to hotlines or helplines for support: only 3% of the 13,945 Malaysian school children between the ages of 7 and 19 who took part in a national survey on cyber safety in 2014 indicated they would seek support via a public hotline for issues related to the internet.[107] Eight children preferred not to say who they disclosed to while another two did not know who they disclosed to.

The household survey also enquired into the reasons why children did not tell anyone about their experiences of OCSEA. These will be discussed under barriers to disclosure and reporting in chapter 2.4.

Accepting Money or Gifts in Exchange for Sexual Images or Videos

When children create sexual content in exchange for something, this constitutes child sexual exploitation, irrespective of whether they are coerced, deceived or actively engage in this activity.[108] The following paragraphs consider the acceptance of money or gifts by children in return for sexual content, regardless of how the process was initiated.

While the practice of accepting money or gifts in exchange for sexual activities is not new,[109,110,111] the use of digital technologies – including by children and young people – to self-produce and send images or videos of oneself in return for money or other material incentives is an emerging trend. One frontline worker indicated that young people influence each other: *"Most of our cases have been influenced by their friends and peers. Currently the victims become more excited because they can earn money for themselves."* (RA3-MY-01-A) This practice could increase the risk of other people sharing someone's sexual images without permission, e.g., 90% of the 'youth-generated' sexual images and videos assessed in a study by the Internet Watch Foundation and Microsoft were 'harvested' from the original upload location and redistributed on third party websites.[112]

Some children and adolescents may also be deceived into generating sexual content. One global platform interviewed for *Disrupting Harm* had observed a trend in Malaysia of children and young people being deceived into sharing self-generated CSAM through modelling recruitment scams.

107. CyberSAFE in Schools (2015) Safety Net: Capacity Building Among Malaysian Schoolchildren On Staying Safe Online. A National Survey Report 2014.
108. ECPAT International (2020). Summary Paper on Sexual Exploitation of Children in Prostitution. Bangkok: ECPAT International.
109. Hasan, H. (2005). Malay Women and Prostitution in Kota Bharu, Kelantan, 1950s-1970s. Journal of the Malaysian Branch of the Royal Asiatic Society, 78(1 (288)), 97–120.
110. Leong, Yee Fong, 'Prostitution in Colonial Malaysia with Special Reference to Penang: Some Preliminary Thoughts', Paper presented at the Penang Story Conference, Penang, 2002 (http://penangstory.net.my/chines-content-paperLeongYeeFong.html).
111. Lim, Lin Lean. (1998). The Sex Sector : the Economic and Social Bases of Prostitution in Southeast Asia. Geneva: International Labour Office.
112. Internet Watch Foundation and Microsoft. (2015). Emerging Patterns and Trends Report #1 Online-Produced Sexual Content.

Given the sensitivity of this topic, only the 15–17-year-old respondents in the household survey were asked whether they had accepted money or gifts in exchange for sexual images or videos of themselves. Among the 524 respondents in this age group, 2% confirmed that they had done so in the previous year. Some children may have been hesitant to reveal their involvement in such activities – even in an anonymised survey – so the true figure could be higher.

Further research is needed to understand the socio-economic context of children's lives to explain these transactions. In addition to poverty, another factor that may increase children's vulnerability to this form of OCSEA is the widespread availability of digital payment systems, including mobile phone payments.

Gaps remain concerning this form of OCSEA. Understanding the intricacies around children's motivations to engage in this practice, their understanding of the risks involved and how they are first introduced to this practice are important questions that require further study.

2.2.1 Potential grooming

Potential grooming – children asked to talk about sex

In addition to the above instances, which represent clear OCSEA, children were also asked in the survey if they had been subjected to certain experiences in the previous year that could be an indication of grooming. Those children who had experienced possible instances of grooming were then asked follow-up questions about the last time that this happened to them, including how they felt, whether it occurred online or offline (or both), who did it to them and whether they told anyone about it. Recognising that sexual exploitation and abuse of children can happen in many different ways and places, most data points below allow for multiple responses and may add up to over 100%.

When the 995 internet-using children in Malaysia who participated in the household survey were asked whether, in the past year, they had been asked to talk about sex or sexual acts with someone when they did not want to, 5% (46 children) said they had received such unwanted requests – with no variations according to age, gender or their location in rural or urban areas. Another 3% of children preferred not to say. In Malaysia, 71% of children – particularly girls and younger children aged 12–13 – and 86% of caregivers considered talking about sex with someone online 'very risky', which may help to explain why some children are reluctant to disclose these experiences.

Depending on the context, these experiences could imply varying levels of harm for the child. For example, a child being asked to talk about sex by a boyfriend or girlfriend but not wanting to engage at that moment might not face serious harm from this interaction. On the other hand, these experiences could also point to malicious instances of attempted grooming; therefore, the figure above is described in this report as an instance of *potential* (versus *actual* or *clear*) grooming.

Online or offline? The 46 children who received unwanted requests to talk about sex in the past year were asked if this most recently happened in person, on social media, in an online game or in some other way. Children were most likely to say this happened on social media (23 children), followed by in person (nine children) and via an online game (seven children). Nine children – mostly children aged 12–14 – said it happened in some other way. Boys were three times more likely than girls to have received the requests in person and almost twice as likely to have received them in an online game. A higher percentage of children living in rural areas received the requests in person than children living in urban areas.

The 23 children who said they most recently received unwanted requests to talk about sex via social media mainly cited WhatsApp (16 children) and Facebook or Facebook Messenger (nine children) as the platforms on which this happened. These were followed by WeChat (six children), TikTok (five children), Twitter (four children), Instagram (four children), Telegram (four children), Snapchat (3) and Flickr (2).

Lesser-known platforms such as Line, Live.me, Twitch and Periscope were respectively cited by two children (all aged 12–13; most of them boys). As observed in other countries, boys received these requests via a wider range of platforms than girls. Similarly, children in urban areas were more likely to receive the requests through a wider range of platforms than children living in rural areas, who mainly received the requests through Facebook, Twitter and WhatsApp. This may partly be explained by the types of online activities that children from urban and rural areas engage in.

The responses captured by this survey question could have included incidents that occurred entirely offline. Similarly, children who complied with the request could have done so without the use of any digital technology. In the following analyses, only the responses of those children who said that they were most recently targeted via social media and/or online games (24 children) have been included. In this way, the focus has been placed on incidents with a digital element, i.e., incidents which might have constituted online grooming and might, therefore, fall within the definition of OCSEA.

How children felt and responded: Eight of the 24 children who had received unwanted requests to talk about sex online (i.e., via social media or an online game) felt embarrassed about the request. Smaller proportions of children felt scared, guilty or annoyed (three children). One child reported feeling distressed. Four children said that receiving an unwanted request to talk about sex did not affect them at all.

Two of the 24 children surveyed for *Disrupting Harm* who received unwanted requests to talk about sex complied with the request, while 12 refused directly. Other tactics used by children included changing their privacy settings (six children), ignoring the person and hoping it would go away or blocking the person (five children), deleting messages from the person concerned (four children), asking the person to leave them alone (three children) or not using the internet for a while (two children).

Base: Internet-using children aged 12–17 in Malaysia from the Disrupting Harm study. n = 995.

Potential grooming – children asked to share sexual images or videos

Some offenders have the intention of manipulating children into self-generating and sharing sexual images or videos through digital technologies, whether or not they also intend to meet the child in person. In 2015, amid concern about this issue, the Lanzarote Committee in charge of overseeing the implementation of the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Abuse (also known as the 'Lanzarote Committee') issued an opinion recommending that states should extend the crime of grooming for sexual purposes to include "cases when the sexual abuse is not the result of a meeting in-person but is committed online."[113]

The children who took part in the household survey were asked whether, in the past year, they had received a request "for a photo or video showing their private parts when they did not want to." While this data could capture requests from partners or peers, it could also point to attempts to manipulate children into self-generating and sharing sexual images or videos through digital technologies. Within the previous year, 3% of the internet-using children surveyed in Malaysia (26 children) had received unwanted requests for a photo or video showing their private parts – with no variations by age, gender or rural or urban location.

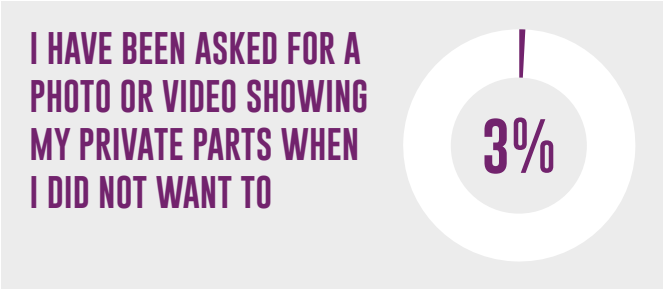
Online or offline? The children who had received an unwanted request to share sexual content were most likely to say this happened online – via social media (13 children) or in an online game (six children). Only two boys aged 12–13 said that they received the request in person. Five children (all aged under 15) said that this happened some other way, while six children preferred not to say.

113. Council of Europe's Lanzarote Committee. (2015). Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Para 20.

The 13 children who received the request on social media cited WhatsApp (nine children), Facebook or Facebook Messenger (five children), Instagram (four children), Telegram (four children), WeChat (four children) TikTok (three children), YouTube (two children), Twitter (two children), Snapchat (two children) and Tumblr (two children). The lesser-known platforms Line, Live.me, Periscope, Twitch and Discord were each also mentioned by two children. While older children aged 16–17 mostly received the requests via WhatsApp, Facebook and WeChat, the youngest children aged 12–13, boys and children living in urban areas cited the widest variety of platforms.

How children felt and responded: Of the 26 children, 13 refused outright. Less direct tactics included ignoring the person concerned (four children), trying to get the person to leave them alone (six children), not using the internet for a while (three children), changing privacy settings (seven children) or blocking the person (three children). Five children – three boys and two girls, all aged under 15 – complied with the request.

While three children said they were not affected at all by the request, the majority reported negative feelings towards the incident, saying that they felt scared (five children), embarrassed (four children), annoyed (four children) and/or guilty (two children).



Base: Internet-using children aged 12– 17 in Malaysia from the Disrupting Harm study, n = 995.

Who made the requests? Among the children in the household survey who had received unwanted requests to talk about sex online and/or to share self-generated sexual content within the last year – indicating that they may have been subjected to online grooming – many said that the requests came from individuals unknown to them. For instance, over half of the children who had received requests to talk about sex online either did not know who had sent it or said that the request came from someone they did not know prior to the incident.

Nevertheless, an important proportion of the children reported that the requests came from someone they already knew – most commonly adult friends or acquaintances, peers under 18 or family members. For instance, six of the 24 children who received requests to talk about sex online said that these requests came from a friend or acquaintance aged 18 and over. Among the 26 children who had received requests to share sexual content, two said the offender was an adult friend while four said it was a friend or acquaintance under 18.

In addition, some of the children preferred not to say who had made the requests. In particular, 10 of the 26 children who had received an unwanted request to share sexual images or videos preferred not to say who the offender was, possibly indicating that the person was known to them.

Disclosure of suspected online grooming

A number of children who had received unwanted requests to talk about sex online or to share sexual images did not tell anyone the last time that it happened. This was the case for 12 of the 24 children who had received an unwanted request to talk about sex online and for nine of the 26 children who had received unwanted requests for sexual images. Boys, older children aged 16–17 and children living in rural areas were more likely not to have told anyone than girls, younger children aged 12–15 and urban children.

The children who did tell someone about the incident were most likely to confide in a friend, a caregiver or a sibling. A few children told a teacher or another trusted adult (doctor, coach, neighbour etc.).

Few children made formal reports about these incidents. Only one child (a boy aged 12–13 who had received an unwanted request to share sexual content) told the police. Barriers to reporting and reasons for not disclosing will be explored further in chapter 2.4.

2.3 OTHER EXPERIENCES OF CHILDREN THAT MAY BE LINKED TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

In addition to the examples of OCSEA and potential grooming already presented, children may be subjected to other experiences online that can be harmful, such as sexual harassment or unwanted exposure to sexualised content. Moreover, these experiences could, in some instances, contribute to the desensitisation of children so that they become more likely to engage in sexual talk or sexual acts – for example, during a grooming process.

Sexual harassment

Nine percent of the internet-using children included in the household survey in Malaysia (91 children) had, within the past year, been exposed to sexual comments about them that made them feel uncomfortable, such as jokes, stories or comments about their bodies, appearance or sexual activities. Children aged 14–15 were the most likely to have been exposed to such comments. There was no variation by gender. While 22% of the children who had been subjected to uncomfortable comments said this did not affect them at all, the majority reported negative feelings, saying they felt embarrassed (26%), angry (16%), annoyed (10%) or scared (6%).

Online or offline? Children were more likely to have been exposed to discomforting sexual comments online – either via social media (40%) or through an online game (21%) – than in person (29%). A higher percentage of younger children aged 12–13 and boys had experienced these comments in person or via an online game than their older peers aged 16–17 and girls, who were mainly targeted on social media.

WhatsApp (56%), Facebook or Facebook Messenger (38%) and WeChat (23%) were the platforms most commonly cited by children who had been exposed to sexual comments on social media. Instagram, TikTok and Telegram were also each cited by about one in five of the children.

Who harasses children? A majority of the 91 children were subjected to sexual harassment by someone they knew. Twenty-three percent of the children – particularly younger children aged 12–13 – cited the offender as being a peer under 18. Adult friends and family members were each cited by 13% of the children. Younger children aged 12–13 were more likely to be targeted by a family member than older children (12–13: 14%; 16–17: 3%). Over a third of the children were harassed by individuals unknown to them – either someone they did not know prior to the incident (14%) or a person they could not identify (21%). Girls were six times more likely to say that the comments were made by someone they did not know before it happened (girls: 24%; boys: 4%).

Whom children told – if anyone: Of the 91 children who had been sexually harassed in the previous year, 42% did not tell anyone the last time it happened. Children aged 16–17 were less likely to disclose than younger children aged 12–13 (12–13: 24%; 16–17: 44%). The children who did disclose were most likely to confide in a friend (23%), followed by a male caregiver (12%), a sibling (12%) or a female caregiver (11%). The youngest children were more likely to confide in a family member or a teacher than children aged 16–17. For instance, 38% of children aged 12–13 told a male caregiver as compared to only 3% of children aged 16–17. Girls were twice as likely to confide in female caregivers than boys (girls: 15%; boys: 7%). None of the children reported to a helpline or the police.

Among the 38 children who did not tell anyone the last time that they were subjected to uncomfortable comments, 14 said they did not think it was serious enough to report, nine – mostly girls – that they did not know where to go or whom to tell, and eight that they were embarrassed or ashamed or that it would be emotionally too difficult. Smaller numbers of children cited feeling that they had done something wrong (four children), fear of getting into trouble (six children) or fear of trouble for their families (four children) as reasons for not telling.

IN THE PAST YEAR

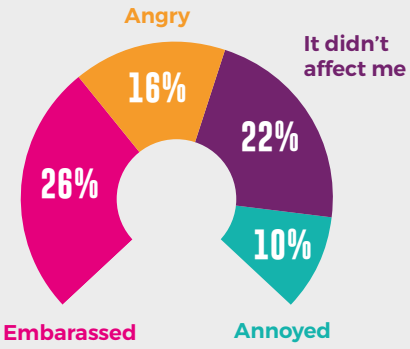
SOMEONE MADE SEXUAL COMMENTS ABOUT ME THAT MADE ME FEEL UNCOMFORTABLE

YES 9%

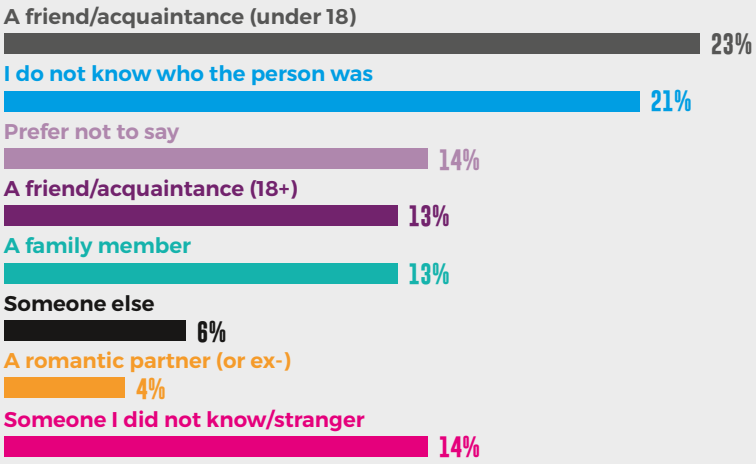
Base: Internet using children 12–17
n = 995 children

THE LAST TIME THIS HAPPENED...

How did you feel?*

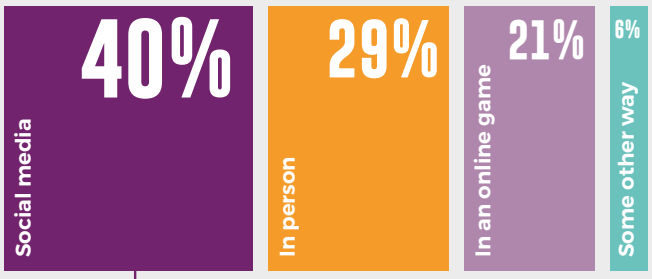


Who did it?*†



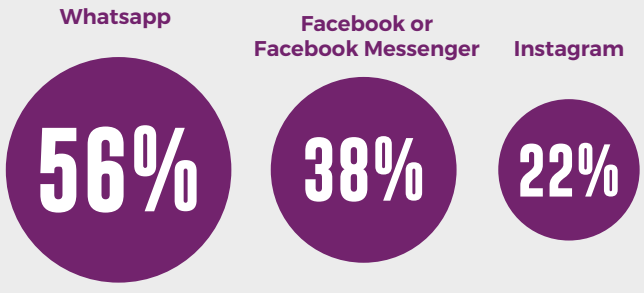
n = 91 internet-using children aged 12–17 who were subjected to verbal sexual harassment in the past year.

Where did it happen?*†



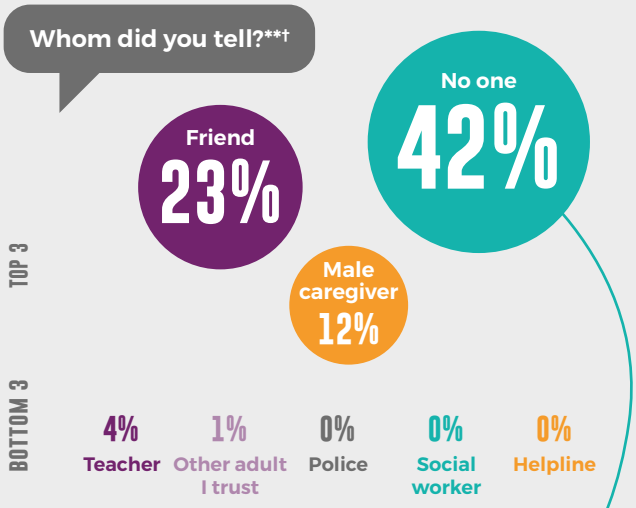
n = 91 internet-using children aged 12–17 who were subjected to verbal sexual harassment in the past year.

On which platform did this happen?*†



n = 36 internet-using children aged 12–17 who were *most recently* subjected to verbal sexual harassment *via social media.*

Whom did you tell?**†



n = 91 internet-using children aged 12–17 who were subjected to verbal sexual harassment in the past year.

Why did you not tell anyone?*†

n = 38 internet-using children aged 12–17 who *did not tell anyone* the last time they were subjected to verbal sexual harassment.

*These figures represent the most common responses selected by children.
**These figures represent the most and least common responses selected by children.
†Multiple choice question

Source: Disrupting Harm data

2.3 OTHER EXPERIENCES OF CHILDREN THAT MAY BE LINKED TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Receiving unwanted sexual images

Among the children surveyed for *Disrupting Harm,* 9% (85 children) said that someone had sent them sexual images or videos that they did not want within the past year. Older children aged 16–17 were somewhat more likely (12%) to have received such unwanted content as compared to younger children (12–13: 7%; 14–15: 7%). Boys and girls were equally likely to have received unwanted sexual content. Most children who had received this content reported negative feelings about the last time this happened, feeling angry (19%), embarrassed (14%) or annoyed (12%). Nine percent – mostly aged 16–17 – felt guilty about having received unwanted sexual images. Seven percent felt scared. Children aged 12–13 were twice as likely to feel scared as children aged 16–17.

The unwanted receipt of sexual images also featured in the survivor conversations with young people who had experienced OCSEA in Malaysia: *"So this is where I started getting to know strangers. I had never used this site, so I didn't know how to operate it and I had never used videocall to chat. So, I started chatting with people my own age – normal conversation like, 'What are you doing'. Then, this guy suddenly showed me his thing. At that time, I was like, 'Eh what's this? I'm going to change to a different chat'. Then he said. 'Wait awhile….'"* (RA5-MY-02)

Online or offline? The vast majority of the children who had received unwanted sexual images received them via social media (64%). Others said it happened via an online game (23%) or in person (15%). Girls and children aged 14 and above overwhelmingly cited social media.

The children who had received unwanted sexual content via social media commonly reported that this happened on WhatsApp (63%), Facebook/Facebook Messenger (38%) or Telegram (19%). WeChat, YouTube and Instagram were also mentioned.

Who sends unwanted sexual content? Half of the children received the unwanted sexual images from individuals unknown to them: 31% still did not know who the sender was, and 19% said that it was someone they did not know before the incident. Children aged 16–17 were twice as likely to be unaware of the sender's identity as children aged 12–13 (12–13:19%; 16–17: 41%). Girls were more likely than boys to report that it was someone they did not know before the incident (girls: 26%; boys: 9%). The easily abused anonymity provided by the internet probably helps to explain why unwanted sexual images are generally sent via social media and why the offender is often someone unknown to the child.

Other children who had received unwanted sexual images received them from people they already knew, including peers under 18 (cited by 20% of the children: 26% of the boys and 12% of the girls), adult friends or acquaintances (9%) and romantic partners (5%). Thirteen percent preferred not to say. These were mostly younger children (12–13: 35%; 16–17: 2%)

Whom children tell – if anyone: Thirty-four percent of the children who had received unwanted sexual content in the previous year did not tell anyone about it. Children aged 16–17 were twice as likely not to tell anybody as children aged 12–13 (12–13: 24%; 16–17: 44%). Among the children who did disclose, friends were the most common confidants (30%). Smaller proportions of children told a sibling (16%), a female caregiver (15%) or a male caregiver (13%). None of the children aged 16–17 told a caregiver. Only one of the 85 children chose to tell a teacher, one told a social worker and one called a helpline, while three reported to the police.

Of the 29 children who did not tell anyone that they had received an unwanted sexual image, many believed it was not serious enough to report (nine children). Others said nothing would be achieved by reporting, they did not know where to go or whom to tell or that they were too embarrassed to tell anyone. The youngest children, aged 12–13, and girls were more likely to say that they did not know where to go or whom to tell as compared with children aged 16–17 and boys (12–13: 50%; 16–17: 12%; girls: 29%; boys: 13%).

IN THE PAST YEAR

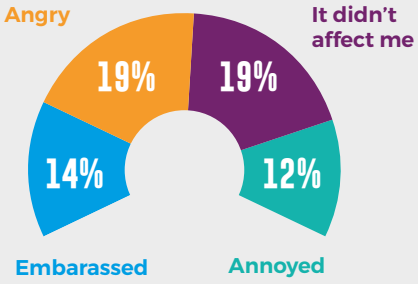
SOMEONE SENT ME SEXUAL IMAGES I DID NOT WANT

YES 9%

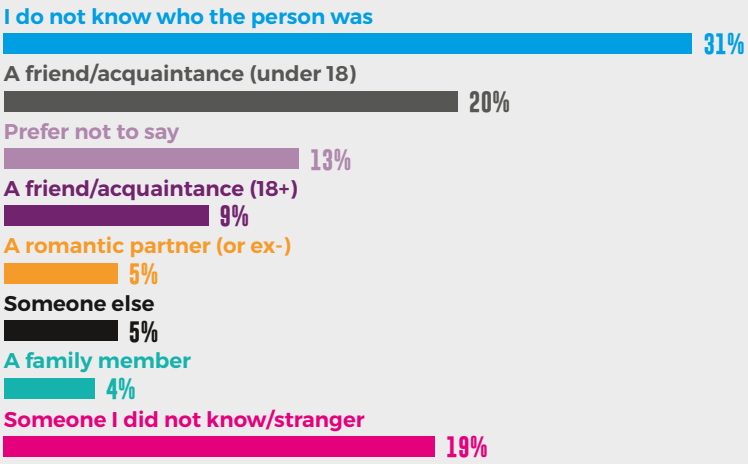
Base: Internet using children 12–17
n = 995 children

THE LAST TIME THIS HAPPENED...

How did you feel?*

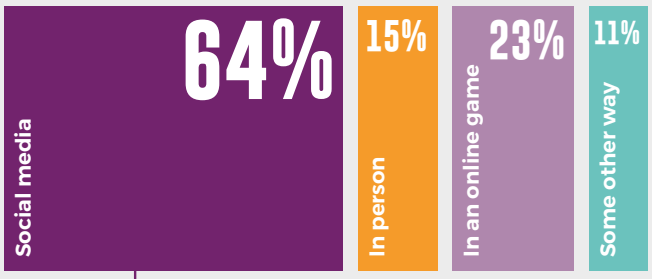


Who did it?*†



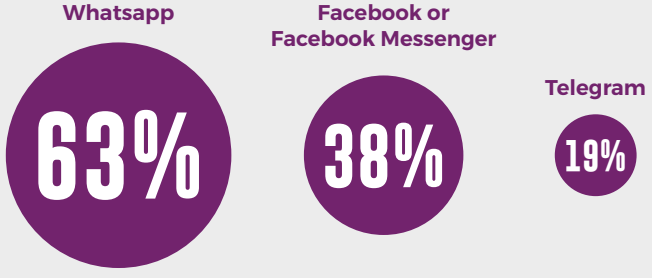
n = 85 internet-using children aged 12–17 who received unwanted sexual images in the past year.

Where did it happen?*†



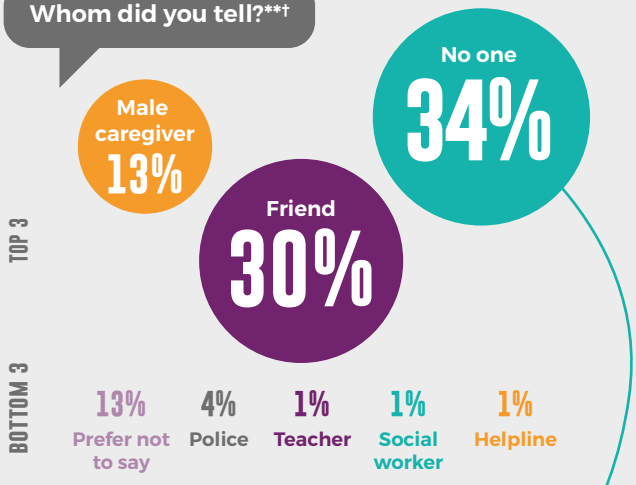
n = 85 internet-using children aged 12–17 who received unwanted sexual images in the past year.

On which platform did this happen?*†



n = 54 internet-using children aged 12–17 who *most recently* received unwanted sexual images *via social media*.

Whom did you tell?**†



n = 85 internet-using children aged 12–17 who received unwanted sexual images in the past year.

Why did you not tell anyone?*†

n = 29 internet-using children aged 12–17 who *did not tell anyone* the last time they received unwanted sexual images.

*These figures represent the most common responses selected by children.
**These figures represent the most and least common responses selected by children.
†Multiple choice question

Source: Disrupting Harm data

The Continuum of 'Online' and 'Offline' Child Sexual Exploitation and Abuse

Interviews and survey data gathered from a range of stakeholders spanning government, the legal system and frontline social service workers suggest that OCSEA is sometimes perceived as a 'new kind of abuse' requiring an entirely new response. However, strictly categorising child sexual exploitation and abuse as 'online' or 'offline' does not accurately reflect the realities of sexual violence that children are experiencing. Accounts from law enforcement interviewed for *Disrupting Harm*, such as the case of a teacher sexually abusing students to later share images and videos of the abuse on social media (see chapter 2.1.1), demonstrate how the online and offline environment sometimes intersect in the continuum of abuse.

Disrupting Harm uses the term OCSEA to refer to all instances of child sexual exploitation and abuse that have an online dimension. This includes:

1. Sexual exploitation and abuse that takes place exclusively in the online environment. For example, an offender may use the online environment to connect with, convince and/or coerce a child to share self-generated sexual content, which may be later shared more broadly.
2. Sexual exploitation and abuse that takes place offline but is facilitated by online digital technologies. For example, an offender may use the online environment to groom a child with the intention of later meeting face-to-face to engage in sexual abuse or exploitation.
3. Sexual exploitation and abuse that is committed offline and then moves online. For example, a child may be contacted and abused in person, but online tools may be used to communicate with and to coerce the child, to capture sexually explicit images or videos and to potentially share the sexual content with others.

These are only a few examples of the dynamic nature of OCSEA and the characteristic fluidity of movement between online and offline sexual abuse and exploitation.

In addition, when frontline workers in Malaysia were asked to identify factors related to children and factors related to society that affect children's vulnerability to general sexual exploitation and that affect children's vulnerability to OCSEA specifically, they typically selected several of the same factors, including dropping out of school, family violence, increased access to technology and the internet, access and exposure to pornography, stigma from the community and taboos around discussing sex and sexuality.

One of the frontline workers surveyed commented: *"There are more similarities with children's vulnerability largely because of their incapacity to face up to the authority figures in their life and physically, they are at the disadvantage."* (RA3-MY-39-A)

It follows that responses to OCSEA must be embedded within the broader child protection system and not handled in isolation. This means that one set of prevention measures is needed that encompasses all types of child sexual abuse and exploitation. It is also necessary for OCSEA victims to benefit from the same services that exist for other child victims of violence. For example, a criminal justice professional interviewed by *Disrupting Harm* noted that, in Malaysia, the One-Stop Crisis Centres offer medical services which could be accessed by children subjected to any forms of child sexual abuse. (RA4-MY-05-A-justice)

Responses to child abuse may, nevertheless, need to be adapted to take into account the way online technology is being used to facilitate abuse and create new forms of abuse. This may mean ensuring that laws clearly encompass all forms and aspects of OCSEA, providing law enforcement authorities with the personnel and equipment needed to investigate the online aspects of crimes, raising public awareness about the online dimension of child abuse, enhancing the digital skills of children and caregivers and engaging with the digital communications industry.

In Malaysia, it emerged from the interviews with government representatives that there are gaps in how mandated government agencies share data on OCSEA during the investigation process. There is also a need to strengthen law enforcement investigations involving the use of digital forensics, which can only be achieved if greater emphasis and priority is placed on these crimes so that more staff can be assigned to the relevant specialised units. Interviews with the law enforcement authorities revealed that, due to the small number of staff at the Malaysian Internet Crime Against Children (MICAC) Investigation Unit, this unit is unable to engage in proactive and covert investigations.

2.4 BARRIERS TO DISCLOSURE AND REPORTING ON ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN MALAYSIA

Children taking part in the *Disrupting Harm* household survey in Malaysia broadly felt that they could depend on their interpersonal networks for help if needed. As many as 92% of children 'agreed' or 'strongly agreed' that a member of their family would help them if they had a problem, and 68% said that they could talk to their friends about their problems. Yet, in practice, as shown in chapters 2.2 and 2.3, up to 50% of children subjected to various instances of OCSEA or other unwanted experiences on the internet did not disclose to anyone. Drawing on data from the household survey, access to justice interviews with children, survey of frontline workers and interviews with government representatives, this chapter explores the immediate reasons as to why children may not disclose, but also why adults may be reluctant to make formal reports. Some of these reasons overlap and are closely related to the social context, shedding light on gaps in knowledge and attitudes that not only obstruct disclosure and reporting but actually increase children's vulnerability to OCSEA.

2.4.1 Shame and stigma

Shame and embarrassment

In the household survey, some of the children who had experienced OCSEA or other unwanted incidents online but did not tell anybody about it said that they had remained silent out of a sense of embarrassment or shame or a feeling that it would be emotionally too difficult. Shame was, for instance, the most commonly cited reason for non-disclosure among children who did not tell anyone about receiving unwanted requests to share sexual images (three out of nine children) and being subjected to sexual extortion (two out of four children).

Two government representatives interviewed for *Disrupting Harm* in Malaysia argued that sex is a sensitive topic in Malaysia. (RA1-MY-08-A, RA1-MY-10-A) This context could help to explain the discomfort that children and adults feel about disclosing and reporting OCSEA or other unwanted sex-related experiences, whether online or offline. According to a government representative: *"There are various types of parents; the subject of child sexual abuse is still taboo with some parents... Awareness has increased but taboo is still there."* (RA1-MY-08-A)

Stigma and victim-blaming

Among the children in the household survey who did not tell anyone about their most recent experiences of OCSEA or about other unwanted sex-related experiences online, common reasons cited for not disclosing included feeling that they had done something wrong, fear of getting into trouble and fear of creating trouble for the family. For instance, among the four children who did not tell anyone about being threatened or blackmailed, two worried about getting into trouble. Similarly, two children who experienced non-consensual sharing of sexual images kept the incident to themselves for fear of getting into trouble or fear of causing trouble for their families. These responses suggest that a child who has experienced sexual abuse may risk being stigmatised.

Children who have experienced OCSEA may feel that they themselves are responsible. In the household survey, 41% of internet-using children aged 12–17 believed they were the ones most responsible for their online safety. Parental attitudes may reinforce these reasons for non-disclosure. Data from the household survey showed that 78% of children and 83% of caregivers believed that it is the victim's fault when a self-generated image or video is shared further. Many children may be unwilling to disclose instances of OCSEA for fear of punishment from their caregivers, including restrictions of their internet use. Indeed, of the caregivers surveyed, 36% stated that, if anything bothered their children online, they would restrict their internet use.

2.4 BARRIERS TO DISCLOSURE AND REPORTING ON ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN MALAYSIA

Shame and stigma may also affect reporting of child abuse by caregivers themselves. When asked what course of action they thought they would take if their child was subjected to sexual harassment, abuse or exploitation, 60% of caregivers said they would tell a spouse and 34% another family member. In contrast, only 13% reported that they would tell a social worker, while 19% would call a helpline. Fifty-five percent of caregivers who would not report if their child was subjected to abuse, exploitation or harassment feared repercussions, while 18% would not report to avoid creating trouble.

In the conversations with young people who had survived OCSEA for the *Disrupting Harm* research, it was evident that they had experienced shame, but also felt that they were blamed for what had happened: *"I didn't know how to handle it, like my Dad was crying and like being sad and disappointed in me because I did stuff with a guy, like he was sad that, I don't even know why he was sad, but I think he was sad about the wrong thing. I think he was asking me like, 'Why did you do that?', when the question should have been like, 'Why did he do that to you?'* (RA5-MY-01)

Stigma and victim-blaming may come from the family or the community. A justice professional from the special court handling Sexual Crimes Against Children told *Disrupting Harm* that children can experience continual harassment and pressure from family members to withdraw complaints and settle the cases outside the court system (see also chapter 3.2.7).

One criminal justice professional said they were *"aware of cases where child victims have to face inappropriate questions in the police station, occasionally made by unethical police officers or investigative officers who would insinuate that the act and blame rest on the child victims as the reason for the cases to have occurred."* (RA4-J-MY-05-A) While this may not be common, such attitudes on the part of law enforcement could contribute to a culture that deters children from coming forward. It is vitally important to educate the public that experiencing abuse is never the child's fault, and that they should not be punished for it.

Stigma when the offender is of the same sex

Under-detection and under-reporting of male child sexual exploitation and abuse is a global problem, resulting from a range of social and legal factors.[114] As global evidence suggests, a child abused by an offender of the same sex may have difficulty reporting the offence due to the stigma associated with homosexuality.[115,116] This barrier to reporting exists both for heterosexual children who experience abuse at the hands of a same-sex offender and for young people with other sexual orientations or gender identities. Male children abused by an offender of the same sex may thus face further difficulty reporting in Malaysia due to the criminalisation of male homosexuality in the current law.[117] Male children may fear legal consequences if they report. In practice, inconsistencies regarding the age of sexual consent, as described in the Overview of Legislation and Policy, may lead to different levels of protection depending on the sex and age of the children involved in the abuse.

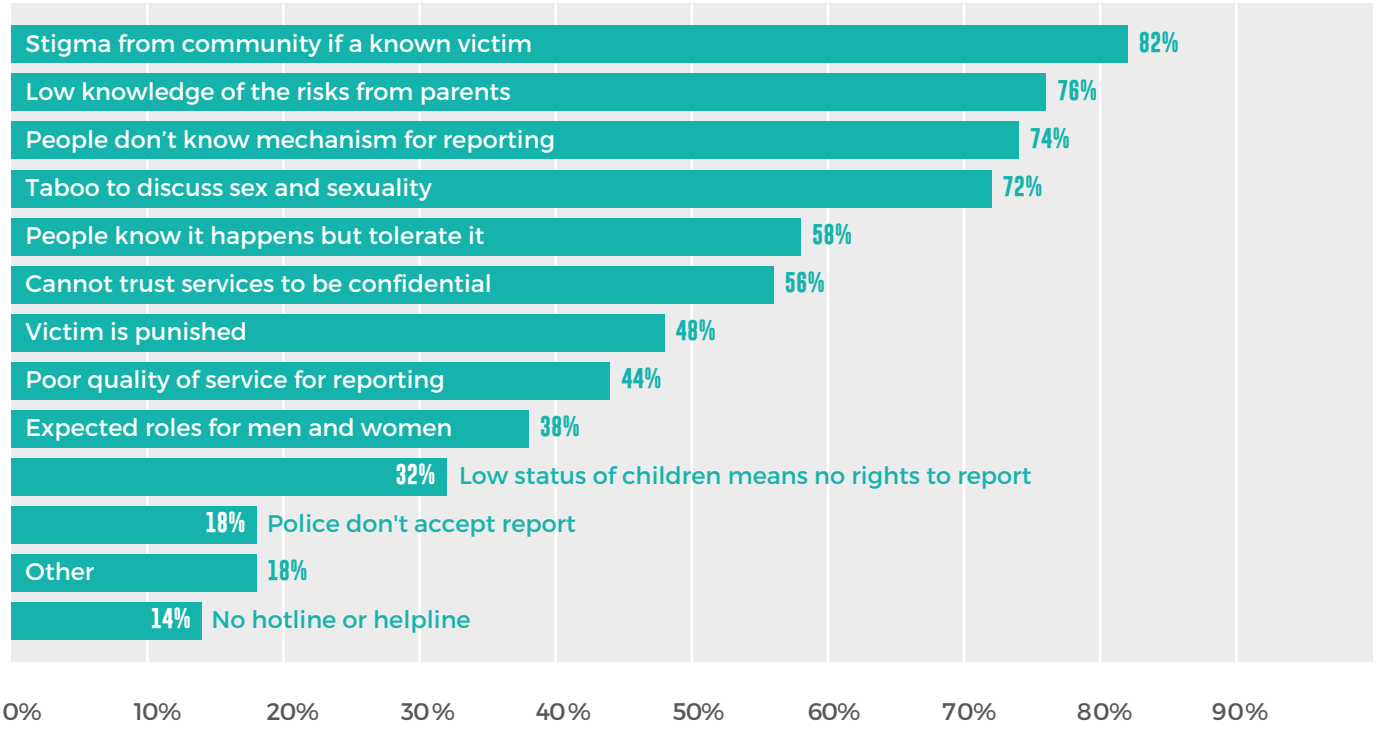
114. Josenhans, V., Kavenagh, M., Smith, S., & Wekerle, C. (2019). Gender, rights and responsibilities: The need for a global analysis of the sexual. Child Abuse & Neglect, 110 (Part 1), 4.
115. Josenhans, V., Kavenagh, M., Smith, S., & Wekerle, C. (2019). Gender, rights and responsibilities: The need for a global analysis of the sexual. Child Abuse & Neglect, 110 (Part 1), 4.
116. United Nations Children's Fund, Research on the Sexual Exploitation of Boys: Findings, ethical considerations and methodological challenges, UNICEF, New York, 2020.
117. Government of Malaysia (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017. Sections 377A, 377B and 377D on Unnatural Offences.

Frontline workers' views on the stigma around and discomfort when discussing sex

The fact that many children subjected to OCSEA do not tell anyone, particularly an adult, can be partly attributed to a common related to discomfort discussing sex and stigma experienced by some victims of sexual crimes. As many as 82% of the surveyed frontline workers believed that stigma from the community influences the reporting of OCSEA in Malaysia – making it the most commonly perceived barrier to reporting. Taboos around sex and sexuality were cited as a barrier to reporting by 72% of the frontline workers (see Figure 30).

A common discomfort related to openly discussing sex and sexuality and stigma around sexual experiences not only hinder disclosure but increase children's vulnerability to abuse and exploitation. When the frontline workers were asked which societal factors increase children's vulnerability to OCSEA, 49 out of the 50 frontline workers reported perceived stigma from the community and taboos around discussing sex and sexuality as the top two factors (Figure 31).

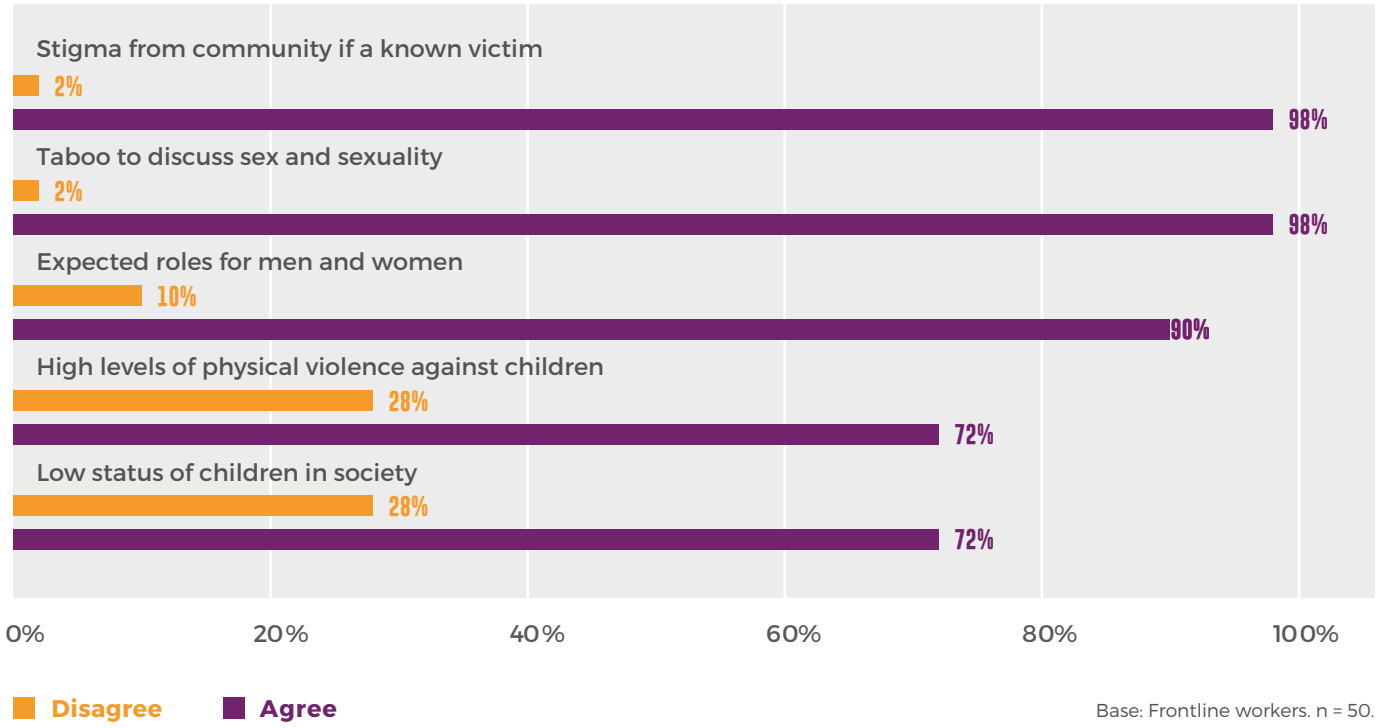
Figure 30: Frontline workers' perceptions of barriers to reporting OCSEA.



Base: Frontline workers. n = 50.

2.4 BARRIERS TO DISCLOSURE AND REPORTING ON ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN MALAYSIA

Figure 31: Frontline workers' perceptions of societal factors that affect children's vulnerability to OCSEA.



Base: Frontline workers. n = 50.

One frontline worker stressed how non-disclosure of OCSEA due to embarrassment about sex and the stigma surrounding children's sexual experiences actually facilitates abuse and exploitation: *"Taboo and stigma may increase the likelihood of suppression to discuss the topic openly in the society, increasing chances of children exploring or being exposed to it silently online, which may make them less protected against exploitation."* (RA3-MY-24-A)

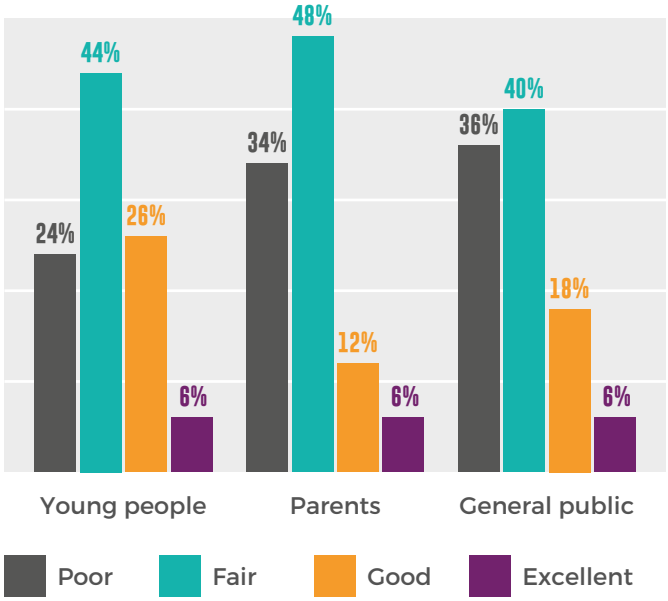
2.4.2 Lack of awareness about OCSEA

Some of the children surveyed who chose not to tell anyone what had happened to them attributed this to the fear that no one would believe them or understand their situation and/or to not thinking the incident was serious enough to report. For instance, thinking the incident was not serious enough to report was the most common reason given by children who did not disclose experiences of sexual harassment (14 out of 38 children) or receiving unwanted sexual content (nine out of 30 children).

A proportion of children who did not report offers of money or gifts in exchange for sexual images (one out of four children) or experiences of non-consensual sharing of sexual content (one out of seven children) said that they worried that no one would believe them. Some children (two out of nine children) were also unaware they could report an experience of online grooming in which they were asked to share sexual content. This may point to a lack of knowledge of what constitutes OCSEA, and how serious it is, both among children and among the people around them.

When the frontline workers surveyed for *Disrupting Harm* were asked to appraise the awareness of young people, caregivers and the general public about OCSEA, the majority rated the awareness of OCSEA among these different groups as either 'poor' or 'fair', as shown in Figure 32.

Figure 32. Frontline workers' perceptions of awareness of OCSEA among children, caregivers and the general public.



Base: Frontline welfare workers. n = 50.

Gaps in awareness about sexual exploitation and abuse, including OCSEA, in Malaysia are partly a reflection of the discomfort around discussing sex and sexuality. Sensitivity about discussing sex extends to discussions of child sexual abuse and exploitation. In the words of a frontline professional: *"I'm not sure if the general population knows about or understands the concept of OCSEA, as we just don't talk about ANYTHING related to sex, what's more when it comes to children."* (RA3-MY-13-A)

A solid understanding of OCSEA-related risks and awareness that OCSEA is a crime are important as they provide a basis for initiating legal action. Children, their caregivers and the general public need to understand what online actions and online content constitute OCSEA. Without this understanding, OCSEA is unlikely to be reported. Aside from hindering disclosure and reporting, a lack of awareness, or perceptions that OCSEA is not serious or harmful to children, may also contribute to harmful attitudes towards abuse, such as victim-blaming (see chapter 2.4.1).

Children's awareness of OCSEA

The household survey indicated that at least 60% of internet-using children aged 12–17 had not received any sex education. This figure was 70% among 12–13-year-olds and 46% among 16–17-year-olds. Only 29% of children indicated that they had received sex education (12–13: 16%; 16–17: 42%). This percentage was 26% in rural areas as compared to 31% in urban areas. Eleven percent of the children did not know whether they had received sex education or preferred not to say.

Access to comprehensive sexuality education: Age-appropriate education on sexual and reproductive health can increase awareness around OCSEA. Teaching children about sexuality, bodily integrity and consent may help them recognise risky situations and inappropriate behaviours both offline and online.

Among the children who had received sex education, 83% stated that much of the information provided pertained to morality. Encouragingly, 71% also reported that the sex education they received discussed assertiveness and how to say 'No'.

Although most children said that they had not received any sex education, one government official stated that Malaysian school children at primary and secondary levels learn *"about the risks of sexual exploitation and sexual abuse and the means to protect themselves through the syllabus of Pendidikan Jasmani dan Pendidikan Kesihatan [Physical and Health Education], Science Education, Islamic Education, and Moral Education."* (RA1-MY-08-A) These differing perspectives perhaps indicate that there is a disconnection between policy regarding OCSEA and the level to which this is perceived as useful by children.

Commenting on disparities in the levels of awareness of OCSEA among children, a frontline professional believed that this *"goes back to education policies; the government needs to be more active and understand the serious impact on the society and community. Young people are looking in all the wrong places to obtain info and support."* (RA3-MY-39-A)

2.4 BARRIERS TO DISCLOSURE AND REPORTING ON ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN MALAYSIA

Sources of information about sex and sexuality: With regard to sources of information about sex and sexuality, 90% of the children reported that schoolteachers were their primary source of information, followed by friends (32%) and mothers (31%). The prominence of caregivers as sources of information appeared to decline with the age of the child: older children aged 16–17 tended to turn to friends, books and magazines, and websites and social media in higher proportions than their younger peers. Similarly, boys and children in rural areas were less likely to seek information from their caregivers and reported looking for information on websites and social media, possibly due to more conservative family norms in rural areas.

One of the surveyed frontline workers worried that unreliable or untrustworthy sources of information might further increase children's vulnerability to OCSEA: *"It is difficult for people in Malaysia to talk about sexual and reproductive health openly, especially for under-age individuals. They [children] tend to get their sexual and reproductive health education online, sometimes from random strangers. This puts the children at risk of being exploited."* (RA3-MY-38-A) Meanwhile, a government official noted: *"Sex is taboo to society; thus educators, parents and community leaders require sensitisation seminars or exposure to accurate information contained in sexual education modules."* (RA1-MY-10-A)

When asked whom they would prefer to receive information about sex and sexuality from, 48% of the children surveyed pointed to schoolteachers.

As many as 22% of children said that they did not want to receive any sex education. Inability and/or unwillingness to learn about sexuality, including consent and bodily integrity, may increase children's vulnerability to OCSEA.

Adults' awareness of OCSEA

Several of the frontline workers suggested that awareness raising is very much needed in the community, and that many people do not yet see online crimes as an issue. In particular, one government representative suggested that *"reaching out to marginalised groups and those in the rural regions is still a problem."* (RA1-MY-10-A)

As seen in Figure 30, 58% of the frontline social service providers surveyed believed that abuse being "tolerated by society" constitutes a barrier to reporting. Recent research on violence against women in Malaysia points to a number of common attitudes that justify, minimise or blame survivors for forms of violence perpetrated against them. Beliefs that domestic violence and physical violence are a normal outcome of stress, frustration, jealousy or anger may, for instance, contribute to shifting blame from offenders to victims. Crucially, such beliefs may infiltrate structures of support for survivors.[118] The data from frontline workers for *Disrupting Harm* suggests that similar attitudes – that abuse can be socially 'tolerated' – may negatively influence disclosure and help-seeking by OCSEA caregivers and that trusted adults hold a critical role in receiving initial disclosures from children and supporting formal reporting. The household survey showed that children subjected to OCSEA and unwanted online experiences were most likely to confide in someone known to them (including their caregivers). In fact, interviews with justice professionals and the threat assessments of law enforcement agencies further indicated that reports were most often made by adults, or by children themselves with the support of an adult. The threat assessment data indicated that victims report such crimes when supported by peers or an adult from their circle of trust.

118. Women's Aid Organisation. (2021). A Study on Malaysian Public Attitudes and Perceptions towards Violence Against Women: A Summary of Initial Findings and Recommendations.

Caregivers' Knowledge of Online Child Sexual Exploitation and Abuse

Limited knowledge concerning the associated risks on the part of parents was considered a barrier to the reporting of OCSEA by 76% of the frontline workers surveyed (see Figure 30). This made it the second most important barrier to reporting after fear of stigma.

However, according to the household survey of internet-using children and their caregivers, 94% of the caregivers had received information about their children's online safety.

When asked about the channels through which they received guidance on how to support their children's internet use and keep them safe, 63% of the caregivers in the household survey mentioned family or friends (see Figure 33). Others cited social media (47%), television (36%) or their children's school (35%) as sources of information. Of note, some respondents identified online parenting apps as sources of information. These were also the channels through which the caregivers said they would prefer to receive guidance. More female caregivers than male caregivers preferred to receive information from family and friends, while the latter said that they would prefer to rely on their child's school or on online safety courses in higher proportions than their female counterparts. These channels could, therefore, be leveraged to disseminate awareness messages or educational programmes about how caregivers can empower children to use the internet safely and effectively.

Caregivers living in rural areas were less likely to rely on social media or online safety courses to obtain information. Some caregivers, particularly older caregivers, named religious leaders as a source of information.

Figure 33: Caregivers' actual and preferred sources of information concerning how to support their children's internet use and keep them safe online.

Source of information	Actual	Preferred
Family or friends	63%	62%
Social media	47%	48%
Television	36%	37%
Child's school	35%	41%
Religious leaders	19%	12%
Online safety course	15%	24%
Radio	14%	15%
Newspapers or brochures	12%	18%
Do not get any information about this	6%	N/A
Other sources	2%	2%
Do not know	3%	3%

Base: Caregivers of internet-using children aged 12–17 in Malaysia. n = 995.

Awareness about OCSEA may be limited among professionals working with children, among caregivers and in the community. One justice actor argued that *"some schools do not know of the existence of this act [Sexual Offences against Children Act] and therefore exposure [awareness raising] of this act must be done in rural areas. Additionally, this will educate these children on OCSEA."* (RA4-J-MY-05-A)

A government representative interviewed suggested that workers in district or community clinics may not be as informed as workers in major hospitals – possibly due to the lack of resources for training and no clear standard operating procedures being in place. (RA1-MY-05-A) One frontline professional appeared to agree: *"I myself lack knowledge and awareness regarding OCSEA. I feel that awareness is drastically needed, especially for those who work directly with children, guardians and schoolteachers."* (RA3-MY-18-A)

2.4.3 Inadequate knowledge of the reporting mechanisms and low confidence in the justice process

Seventy-four percent of the frontline workers surveyed agreed that a lack of knowledge of the reporting mechanisms was a barrier to the reporting of OCSEA in Malaysia (see Figure 30).

In the household survey, it was common for those victims of OCSEA, or children experiencing incidents that might have been indicators of OCSEA, who had not told anyone to say that they did not know where to go or whom to tell. This was mentioned by three out of the four children who had not opened up about been offered money or gifts in exchange for sexual images, two of the four children who had not told anybody about being subjected to sexual extortion and seven out of the 12 children who had remained silent after being asked to talk about sex.

"Not knowing where to go or whom to tell" suggests that the children were hesitant to confide in the people around them, but, at the same time, were insufficiently familiar with the formal reporting mechanisms, such as helplines, the police and the social media platforms that they were using. In fact, 56% of all the children surveyed said that they did not know where to get help if they or a friend were subjected to sexual harassment or abuse. With respect to online reporting, 34% of the children surveyed did not know how to report harmful content on social media. Furthermore, in all cases of OCSEA, potential OCSEA or other unwanted incidents covered by the household survey, only very small proportions of children actually made use of these formal reporting mechanisms.

The *Disrupting Harm* data indicates that children undergoing OCSEA are more likely to tell their caregivers than to go directly to formal reporting mechanisms. The caregivers themselves might also not be aware of the reporting mechanisms. When asked what course of action they would take if their child was bothered by something online, only 22% of the caregivers included in the household survey said that they would report it to a helpline, many indicating instead that they would seek help or advice from friends and family (48%).

A law enforcement representative suggested that it may be prudent to raise public awareness on the mandatory reporting legislation (see below) and on OCSEA itself: *"I don't think the general public is fully aware that there is this mandatory obligation to lodge a report for cases of child sexual exploitation. I think we have to increase awareness on this particular section, for the public to fully understand the Act."* (RA4-J -MY-09-A)

Even when reporting mechanisms are visible and accessible, disclosure and reporting of OCSEA may be hindered by low confidence in the reporting process or the justice system. In the household survey, six out of the 29 children who did not disclose that they had received unwanted sexual content said that they did not believe that anything would be done about it. Three of the thirty-eight children who had experienced sexual harassment and not told anybody cited fear that the incident would not be kept confidential. Similar considerations may also affect the likelihood of caregivers making official reports of abuse.

The reasons given by the 11 caregivers in the survey who said that they would not report sexual harassment, exploitation or abuse of their children included fear of not being treated properly (one caregiver), fear of negative consequences (one caregiver), the expectation that it would take time and money (one caregiver) and a belief that reporting would not change anything (one caregiver). Six of the caregivers feared repercussions and two said that they would not report to avoid creating trouble. Consequently, the non-reporting of OCSEA by adults is not always due to a lack of knowledge of OCSEA or of the channels for reporting it; it also relates to issues of stigma and/or confidence in the authorities.

One justice professional interviewed for *Disrupting Harm* identified the tediousness of the reporting process as a barrier to reporting. An NGO representative taking part in the access to justice interviews elaborated as follows: *"The reporting process is very long. We go up to seven and a half hours. The shortest was about one hour. So, it varies and is dependable on different police stations as well."* (RA4-J-MY-07-A)

Even when reporting mechanisms are visible and accessible, disclosure and reporting of OCSEA may be hindered by low confidence in the reporting process or the justice system [...] Similar considerations may also affect the likelihood of caregivers making official reports of abuse.

3. RESPONDING TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN MALAYSIA

This chapter presents evidence concerning current response mechanisms to OCSEA in Malaysia, including the formal reporting options and the responses of law enforcement authorities and the court system. The contributions that government, civil society and the internet and technology industry make to combating OCSEA in Malaysia are also assessed. This chapter draws on the testimonies of individuals working in the criminal legal system (law enforcement officials and prosecutors), legal aid societies, NGOs, frontline workers and private practitioners regarding access to justice and legal remedies in Malaysia (interviewees are referenced as RA4-MY-XX-A-justice). Much of the evidence presented in this chapter is drawn from qualitative interviews and the responses may not reflect the full range of experiences of those accessing the response mechanisms to OCSEA in Malaysia.

3.1 FORMAL REPORTING MECHANISMS

3.1.1 Reporting and referral to law enforcement agencies

Who reports?

As seen in chapter 2, children who are subjected to OCSEA or other unwanted experiences online are much more likely to confide in someone known to them (including their caregivers) than to report directly to the police or a helpline. Not a single child in the household survey had reported to a social worker. Interviews with justice professionals and the threat assessment conducted with the law enforcement authorities also indicated that cases were typically reported to the authorities by adults, or by children themselves with the support of an adult from their circle of trust.

As one respondent from the special court handling Sexual Crimes against Children indicated: *"Usually [complaints are made] by the parents themselves, but we also have teachers, counsellors from the schools or headmasters and medical officers."* (RA4-J-MY-10-A) Similarly, criminal justice professionals stated that complaints were typically made to law enforcement units on children's behalf by caregivers, other family members and medical, educational and social welfare professionals.

Interestingly, the OCSEA cases investigated by the Royal Malaysia Police D11 division between 2017 and 2019 were reported by members of the public.

Figure 34: How cases are reported.

	2017	2018	2019
Family or friends	10	9	15
Social media	0	1	0

Base: D11, Division of the Royal Malaysia Police.

Despite their vulnerabilities, the children – with the help of an adult – were able to report the offence to the law enforcement authorities. Although the offenders had calculated strategies for normalising abuse, which involved, for instance, grooming the victim and/or showing pornographic images and video content, the victims still realised that they were being abused and summoned the courage to report the cases.

Some of the justice professionals interviewed noted that complaints can also be made on behalf of the children by a variety of public and private organisations, for example, the Attorney General's office and the Human Rights Commissioner. One justice professional said that NGOs play a critical role in reporting by supporting and educating children and the wider public on their mandatory reporting duties. (RA4-J-MY-06-A) INTERPOL research activities revealed that the Office of the Child Commissioner, which has four staff members dedicated to children's rights, registers complaints and requests information about procedures from law enforcement departments in order to help children access the justice system.

> "Usually [complaints are made] by the parents themselves, but we also have teachers, counsellors from the schools or headmasters and medical officers."

Mandatory Reporting Legislation

The Child Act of 2001 imposes mandatory duties on professionals working with children to report incidences in which child sexual abuse, including OCSEA, is thought to be occurring.[119] The professionals are obliged to report these incidences to social welfare officers, who then step in to ensure that the children receive the proper medical care and engage with the correct reporting mechanisms.[120] Violation of this provision is punished by a fine not exceeding RM5,000 (approx. US$1,135 as of June 2022), imprisonment for a term not exceeding two years, or both.[121]

In addition to the Child Act of 2001, the Sexual Offences against Children Act imposes a more general mandatory reporting duty that requires private citizens to report any offence outlined in the act (which includes OCSEA).[122] The consequences for not reporting can be punishable with a fine of up to RM5,000. [123]

A government representative and a justice professional indicated that both pieces of mandatory reporting legislation are known, especially among professionals who work with children. (RA1-MY-07-A&B) However, one law enforcement representative suggested, with regard to the Sexual Offences against Children Act, that the *"general public is still not fully aware that there is a mandatory obligation for reporting child sexual abuse cases."* (RA4-J -MY-09-A) The representative further recommended that more awareness should be raised among the general public about their responsibilities under the act and the consequences of non-compliance.

A discussion of mandatory reporting and Internet service providers can be found in chapter 3.5.2. There are no mandatory reporting obligations for Internet service providers in the Multimedia and Communication Commission Act.

The role of social welfare officers

As suggested by the mandatory reporting obligations for professionals,[124] social welfare officers play a key role in the formal reporting process. Justice professionals interviewed for *Disrupting Harm* explained that, once a report is made to a social welfare officer, the officer should take the victim to a hospital for medical attention and refer the case to the police for further action. Two government representatives and several justice professionals interviewed for *Disrupting Harm* expressed their belief in the central role that these officers play.

3.1.2 Hotlines and helplines

Child Helplines and CSAM Hotlines: What is the Difference?

The channels through which children and adults can report cases of OCSEA include CSAM hotlines and child helplines. CSAM hotlines focus on working with industry and law enforcement agencies to take down content, and they are now more often accessible by web than by phone. The child helplines provide immediate crisis support, referrals and ongoing counselling and case management services; they generally tend to respond to a broader range of child protection concerns, although some focus specifically on OCSEA.

Hotlines and helplines are another way in which individuals can make formal reports of OCSEA. Typically, hotlines focus on working with the industry and law enforcement agencies to take down content, and nowadays, they typically use a web-only format rather than phone numbers. On the other hand, helplines tend to respond to a broader range of child protection concerns, although some may focus specifically on online child sexual exploitation and abuse. Helplines can provide immediate crisis support, referrals and/or ongoing counselling and case management services.

119. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001, as amended in 2017, Sections 27, 28 and 29.
120. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001, as amended in 2017, Section 27 (1).
121. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001, as amended in 2017, Section, Section 27 (2).
122. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 20.
123. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 20.
124. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001, as amended in 2017, Section 27 (1).

The desk review in Malaysia revealed that government entities and NGOs offer hotline and helpline services (see Figure 35).

Figure 35: Hotlines, Helplines and Portals Relevant to OCSEA Victims in Malaysia.

Government-run	Civil society-run helplines, hotlines and portals
The Talian Kasih 15999 hotline (originally Talian Nur) (Ministry of Women, Family and Community Development)	**Internet Watch Foundation (IWF) – Malaysia**
Cyber999 (Ministry of Communications and Multimedia)	**The Protect and Save the Children Hotline**
Content Forum (Ministry of Communications and Multimedia)	**Lapor Predator Reporting Portal**

Helplines

The Talian Kasih 15999 hotline (originally Talian Nur): Since 2004, the Ministry of Women, Family and Community Development has been a leading government entity in the area of child protection and child development policies in Malaysia. This agency operates a helpline known as Talian Kasih that creates 'NUR Alerts' – alerts that streamline information regarding missing children or victims of abuse and exploitation directly to law enforcement agencies for further action.[125] This helpline is not exclusively dedicated to children but also receives calls from other vulnerable people/adults.[126]

The Talian Kasih 15999 hotline is a 24-hour hotline available for children and adults to report child abuse, bullying and neglect. The hotline aims to automatically divert children for support to a local government social worker/child protector.[127] Using the DiGi telecommunications company services is free.[128]

In an address to the Upper House of Malaysia's Parliament, the Minister of Women, Family and Community Development stated that Talian Kasih received a total of 85,948 calls between May 2015 and November 2019. The highest volume of calls related to child abuse (4,900 cases), followed by domestic violence (3,169 cases).[129] No specific information could be found about how many calls were related to OCSEA.

The Protect and Save the Children Hotline: Protect and Save the Children is an NGO that is said to be the only social organisation in Malaysia that focuses solely on the issue of child sexual abuse.[130] At the time of data collection, the organisation was engaged in education for professionals, community organisations and children. Moreover, it provided treatment – including counselling and therapy services for individuals and groups – and advocacy for policy and legislative changes. During this period, Protect and Save the Children maintained a Monday–Friday hotline and provided a 24-hour SMS/WhatsApp service phone number on its website.[131]

Lapor Predator Reporting Portal: According to its website, Monsters Among Us: Youth Advocates is a youth-led national organisation in Malaysia known for its work combating child sexual abuse.[132] It operates in a variety of ways to advocate, empower, educate and support child victims of abuse. It has an online reporting portal for victims called Lapor Predator.[133] Lapor Predator launched a Chatbot function so that victims of OCSEA can report their experiences more easily and receive support throughout the reporting process, thus helping to streamline the journey from harm to access to justice. Through the Lapor Predator website, the organisation advocates for greater multi-stakeholder collaboration to improve the 'unclear' reporting process for children in Malaysia.

125. ITU. (n,d) Child Online Protection: Malaysia.
126. UNICEF (December 2020) Avoiding a Child Welfare Crisis: Mitigating the Impact of COVID-19 through Social Service Workforce Strengthening.
127. ITU. (n,d) Child Online Protection: Malaysia.
128. UNICEF. (n,d). Report Abuse.
129. Government of Malaysia. (2019). Penyata Rasmi Parlimen Dewan Negara.
130. Protect and Save the Children. (n,d) About Us.
131. Protect and Save the Children. (n,d) About Us.
132. Monsters Among Us: Youth Advocates. (n,d). Who we are.
133. Monsters Among Us: Youth Advocates. (n,d). About Lapor Predator.

CSAM hotlines

The Cyber999 Help Centre and Content Forum: The Ministry of Communications and Multimedia regulates the communication and multimedia sectors. The Ministry assists the Royal Malaysia Police by blocking access to websites containing child sexual abuse materials and helping with suspect identification and digital forensic analyses. Housed within the Ministry of Communications and Multimedia, CyberSecurity Malaysia (which includes MyCERT)[134] and the Communications and Multimedia Content Forum,[135] which fall under the purview of the Malaysian Communications and Multimedia Commission, both work to provide accessible avenues for public assistance regarding cybersecurity matters and reporting inappropriate content.

MyCERT provides assistance in the form of the Cyber999 Help Centre, a resource that is available via an online form, email, SMS, phone calls (from 8:30am to 5:30pm), fax, a mobile app and on a walk-in basis, to help address any concerns regarding computer security and cyberattacks.[136]

A threat landscape analysis conducted by MyCERT in 2019 revealed that 365 incidences of cyber harassment were reported to MyCERT in 2018.[137] Other analysis reports from MyCERT indicate that less than 442 were reported in 2015 and 529 in 2016.[138] No specific information could be found concerning how many reported incidents were related to OCSEA.

International Watch Foundation's Malaysia reporting portal:[139] The International Watch Foundation's reporting portal for CSAM was launched in Malaysia in 2020. No information could be found on how many images have been reported to the portal since its launch.

Perceptions of hotlines and helplines

While there are several hotlines and helplines in Malaysia for children wishing to report OCSEA, the public, including children, may not be aware of these avenues or sufficiently willing to use them.

In 2014, CyberSAFE in Schools (a joint awareness programme run by DiGi Telecommunications, Malaysia Communications and Multimedia Commission, Cybersecurity Malaysia and the Ministry of Education) conducted a national survey on cyber safety with a representative sample of 13,945 Malaysian school children between the ages of 7 and 19 taking part in CyberSAFE in Schools workshops.[140] In this survey, the children indicated their preference for disclosing information about negative experiences and cyberbullying to parents, friends and siblings rather than through other avenues such as childcare professionals or public helplines. Only 3% of the children indicated that they would seek support from a public hotline for issues related to the internet. This is consistent with the findings of the *Disrupting Harm* household survey, i.e., of the children who had experienced OCSEA in the previous year, only one reported the incident to a helpline. Similarly, as seen in chapter 3.1.2, only one of the cases recorded by the D11 division of the Malaysian National Police stemmed from a helpline call.

In a 2019 report, the UN Human Rights Council commented that it was unclear how accessible hotlines in Malaysia are to children in the most precarious situations, including undocumented children and those living in rural and isolated areas.[141]

134. CyberSecurity Malaysia. (n,d) Corporate Overview.
135. Communications and Multimedia Content Forum of Malaysia. (n,d). Fact sheet.
136. MyCert. (n,d). Portal.
137. MyCert (2019). Malaysia Threat Landscape 2018 – Based on Incidents Reported to CyberSecurity Malaysia.
138. MyCert (2017). Incident Trend Analysis for 2016.
139. IWF. (n,d). IWF Malaysia Reporting Portal.
140. CyberSAFE in Schools (2015). Safety Net: Capacity building Among Malaysian schoolchildren on staying safe online: A national survey report 2014.
141. UN Human Rights Council (2019, January 17). *Visit to Malaysia - Report of the Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse.*

3.2 LAW ENFORCEMENT RESPONSE

This section focuses on the capabilities of the law enforcement agencies in Malaysia to prevent and respond to cases of OCSEA. It is primarily based on interviews conducted by INTERPOL with law enforcement units. The findings are complemented by data from interviews with government representatives, frontline social support workers and relevant criminal justice professionals.

3.2.1 Law enforcement/investigative entities and capacities

D11 Division of the Royal Malaysia Police

In Malaysia, the main law enforcement entity that investigates all forms of online and offline child sexual exploitation and abuse is the D11 division of the Royal Malaysia Police (also known as the Sexual, Women and Child Investigation Division). According to INTERPOL research activities, there are a total of 46 officers in the D11 division, 17 of whom are based in the Bukit Aman National Headquarters. These 17 officers are divided into several units within the D11 division and are led by a senior female officer with the rank of Assistant Commissioner of Police. The units are as follows:

- The Sexual Investigation Unit;
- The Child Investigation Unit;
- The Domestic Violence Investigation Unit;
- The Advocacy/Management Unit;
- The Victim Care Centre/Child Interview Centre;
- The Malaysia Internet Crime Against Children (MICAC) Investigation Unit.

The Malaysian Internet Crime Against Children Investigation Unit operates at the national level and specialises in the investigation of cases pertaining to OCSEA.

The Malaysian Internet Crime Against Children (MICAC) Investigation Unit

The Malaysian Internet Crime Against Children Investigation Unit is headed by an Assistant Superintendent of Police and includes four officers dedicated to addressing OCSEA at the national headquarters. These officers are trained to investigate OCSEA cases. The unit also receives and triages CyberTips from the U.S. National Center for Missing and Exploited Children (NCMEC) for Malaysia. There are currently no officers at the state and district levels.

Interview responses clearly indicated that Malaysian Internet Crime Against Children Investigation Unit officers were selected for their experience and expertise, computer skills and backgrounds in cyber-enabled crimes. One government representative said that the unit has been provided with the latest technology to oversee all internet-related media used by offenders to upload, share and promote child sexual abuse materials. (RA1-MY-11-A) However, the unit is not currently equipped to undertake covert investigations and the small team of officers are unable to pursue proactive investigations. The interview responses clearly articulated that the Malaysian Internet Crime Against Children Investigation Unit (and the D11 division in general) has unmet training needs in the areas of covert investigations, open-source intelligence gathering and proactive surveillance techniques.

The Malaysian Internet Crime Against Children Investigation Unit is also known for conducting capacity building programmes, which include courses organised for all D11 officers across the country. In addition, the Malaysian Internet Crime Against Children Investigation Unit is responsible for the monitoring and analysis of trends in offences. A secure, stable, dedicated internet connection was established in September 2021, greatly enabling the unit's work. The unit is staffed by officers who understand Malaysia's legal framework and who are capable of collaborating with foreign law enforcement agencies.

Other investigative entities within the Malaysian government

In addition to the D11 division and its Malaysian Internet Crime Against Children Investigation Unit, government representatives and justice professionals interviewed for *Disrupting Harm* indicated that the Malaysian Communications and Multimedia Commission (MCMC) and the Ministry of Women, Family and Community Development have capacities that contribute to law enforcement responses to CSEA and OCSEA. According to government interviewees, MCMC has 20 investigating officers and an additional forensic team that can be used to support law enforcement agencies when technical assistance is required, including in OCSEA cases. (RA1-MY-02-A&B) The digital forensics department of the Malaysian Communications and Multimedia Commission consists of four units: quality assurance, operations (child online cases are handled by this unit), network, and first responders. The department reports to the head of compliance, who then reports to the chairman of the Malaysian Communications and Multimedia Commission.

Personnel considerations

Malaysia demonstrates political will and preparedness to address OCSEA. However, the law enforcement system needs to prioritise OCSEA so that an adequate number of appropriately trained staff can be assigned to the relevant specialised units. Aside from the low number of staff, there are frequent transfers and reassignments of duties and responsibilities.

3.2.2 Enhancing the response: training, support and development

Training

The Office of the Children's Commissioner; SUHAKAM, which is an independent office responsible for securing and protecting children's rights as outlined in the UN Child Rights convention; the Office of the Deputy Prosecutor, under the Office of the Attorney General's Chamber reporting directly to the Prime Minister; the Principal Assistant Director of the D11 division of the Royal Malaysian Police and the Director of Digital Forensics at the Malaysia commission for Multimedia Communication agreed that OCSEA is an emerging crime area and that it is vital to provide frontline officers with upskilling opportunities. Regular capacity building activities would enable them to perform their duties efficiently and effectively.

The Anti-Human Trafficking and Migrants Smuggling Prevention Division (D3) has organised seminars and workshops with relevant departments of the Royal Malaysia Police in order to enhance the knowledge and preparedness of their staff.

Aside from events organised by foreign law enforcement agencies/organisations, the D11 respondents stated that they organise, co-host and participate in seminars and symposia among themselves and with relevant stakeholders in order to share good practices, success stories and lessons learned from previous cases.

Nevertheless, government representatives and justice actors who were interviewed considered that the training of law enforcement staff on OCSEA is currently insufficient. (RA1-MY-11-A; RA4-J-MY-06-A) Reference was frequently made to the need for training that would help to improve the use of child-sensitive methods. A representative of the Women's Aid Organisation suggested that some training in their programme area already exists for all members of the criminal justice community, including law enforcement agencies, but that the latter, in particular, were in need of further training. (RA4-J-MY-05-A) Several interviewees raised concerns about the transfer of sufficiently trained officers to other departments upon the completion of specialised training. (RA4-J-MY-05-A; RA4-J-MY-07-A; RA4-J-MY-07-B; RA4-J-MY-10-A)

Psycho-social support for police officers

All relevant units acknowledged the need for psychological support, particularly the Malaysian Internet Crime Against Children Investigation Unit. The interviews indicated this is an unmet need and continues to be a significant challenge in intelligence gathering and evidence building. The officer responsible for reviewing CSAM was reported to be suffering from post-traumatic stress disorder. Psychological support would directly enhance the investigative capacities of the specialised unit/team.

Cyber security strategy

The Malaysia Cyber Security Strategy for 2020–2024 promises to enhance the capacity and capability of law enforcement agencies to tackle cybercrime in general, which should have a positive effect on capacities for addressing OCSEA. Under the strategy, a National CyberCrime Enforcement Plan is to be adopted, which will include efforts to increase the knowledge and skills both of law enforcement officers and members of the judiciary and legal professions in the increasingly complex realm of cybercrime.[142]

3.2.3 Equipment

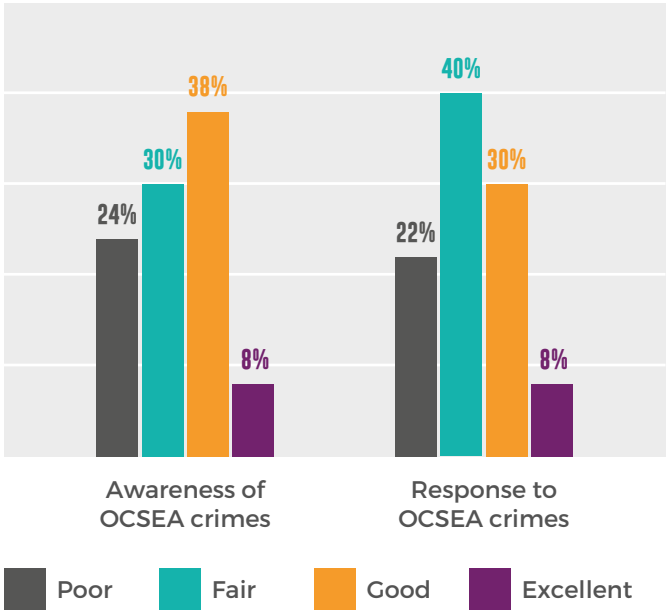
All the respondents in the law enforcement capacity assessment had basic office equipment. However, they regarded low internet broadband speed and poor connections as a challenge that hampered the prompt investigation of cases. According to one government representative: *"[The] lack of information communication technology infrastructure, special equipment, and laptops at all levels is another big challenge for D11."* (RA1-MY-11-A) As previously noted, a high-speed connection was established for the unit in late 2021.

3.2.4 Perceptions of law enforcement awareness and response

When asked about their perceptions of the awareness and response of law enforcement agencies to OCSEA, most surveyed frontline workers described the level of awareness as good (38%) and the response as fair (40%) (see Figure 36). This is a slightly more positive result than perceptions among frontline workers in other Southeast Asian target countries. However, room for improvements remains.

I have had an experience myself lodging a report to the police regarding an OCSEA crime," explained one frontline worker. *"The inspector in charge was not aware of the different social media used, the lingo used by children and lacked important knowledge that an inspector needs to know to execute an effective investigation."* (RA3-MY-42-A)

Figure 36. Frontline workers' perceptions of law enforcement awareness and response to OCSEA-related crimes.



Base: Frontline welfare workers. n = 50.

The justice professionals interviewed shared the perception of a gap between the law enforcement agencies' awareness of OCSEA and their response. A justice professional, who works for a non-governmental organisation that supports victims of OCSEA commented: *"After 17 cases were reported by our clients, it is disappointing to know that there were no further follow-ups for 16 of the cases. The one case that was followed up by the police, was done so only after the parents of the victim had called them."* (RA4-J-MY-07-B) This respondent also noted that status reports on a case can be requested under Section 107A of the Criminal Procedure Code.[143]

142. National Cyber Security Agency. (2020). Malaysia Cyber Security Strategy (MCSS) 2020-2024. Government of Malaysia.
143. Government of Malaysia. (1935). Laws of Malaysia – Act 593 - Criminal Procedure Code, as amended in 2012, Section 107.

3.2.5 Collaboration and coordination between law enforcement agencies and other entities

Intra-government collaboration

The Malaysia Internet Crime Against Children Investigation Unit was reported to work closely with other law enforcement divisions and government agencies. Specifically:

- The *Malaysian Communications and Multi-Media Commission* and the Royal Malaysia Police were believed by one government representative to have formed an internal committee to discuss matters related to enforcement, including content enforcement. (RA1-MY-02-A&B)
- The *National Cybersecurity Agency* provides digital forensics services to law enforcement agencies such as onsite evidence preservation, evidence analysis, professional training and expert witnesses in court proceedings under Section 399 of the Criminal Procedure Code. (RA1-MY-09-A, B & C) *"When it comes to photos, audio or video, we can do the forensics to ensure that it is authentic and to be a part of the evidence. The technical support in the digital forensic department has been mandated and given the recognition as an expert witness in court under Section 399 of the Criminal Procedure Code."* (RA1-MY-09-A, B & C)

Malaysia's national child sex offender registry took effect in April 2019. The registry enables employers to check whether an (potential) employee has committed any sexual offence against children.[144] One interviewed justice actor was of the opinion that *"the sex offender's registry should be made public."* (RA4-J-MY-01-A), while the law enforcement officers interviewed for *Disrupting Harm* all agreed that a system should be put in place to mandatorily and consistently screen prospective employees, including volunteers and disaster relief and humanitarian aid workers, against a registry of child sex offenders.

Interactions with INTERPOL and connection to the International Child Sexual Exploitation database

In 2019, Malaysia was connected to INTERPOL's International Child Sexual Exploitation database[145] and the Malaysia Internet Crime Against Children Investigation Unit was trained in victim identification. The database, which allows investigators from 68 countries to exchange information and share data on cases of child sexual abuse, is an invaluable tool for law enforcement.[146] One government representative confirmed that the D11 division has *"access to the International Child Sexual Exploitation image and video database via the Malaysian Internet Crime Against Children Investigation Unit."* (RA1-MY-11-A) However, as a result of transfers and changes of personnel, the unit does not engage with the database. INTERPOL is working towards renewing this connection and retraining the team in victim identification and the use of the database.

Collaboration with foreign law enforcement agencies

The Malaysia Internet Crime Against Children Investigation Unit is working closely with foreign law enforcement agencies such as the National Crime Agency in the UK, the Federal Bureau of Investigation, Homeland Security Investigations in the United States and the Australian Federal Police on referral cases and joint investigations for transnational cases. One example involved a suspect known to have been in Taiwan while the victims were in Malaysia. The conduit between the two admitted upon interrogation that she had had contact with the suspect in Taiwan. As a result, a report was lodged against the suspect.

One government representative stressed that the law enforcement agencies must make use of these international connections as much as possible to combat OCSEA as *"child sexual offences have increasingly evolved into a borderless crime and therefore require international cooperation."* (RA1-MY-02-A&B)

144. Asia Times Staff (2019). Malaysia launches child sex offender's registry, Asia Times.
145. ECPAT International. (2019). Briefing Paper: Sexual Exploitation of Children in Malaysia.
146. INTERPOL. (n.d.) International Child Sexual Exploitation database.

Collaboration with the financial sector

The emerging commercial nature of OCSEA entails the use of new payment technologies for the sale and purchase of material. Digital currencies, for example, remain largely unregulated. Cooperation with the financial sector and fintech institutions is required in such cases. INTERPOL found that, in Malaysia, there is a system in place to retrieve pertinent data from private sector companies such as banks and financial institutions. In the course of an investigation, the relevant law enforcement units are able to reach out to the financial sector to request specific intelligence. The financial sector often shares information with the police (the D11 division), the Office of the Child Commissioner Human Rights Commission and the Deputy Prosecutor at the Attorney General's Chambers.

3.2.6 Law enforcement efforts to create a child-friendly process

Interaction between support services and law enforcement

All interviewees from the law enforcement sector expressed their commitment to a victim-centred approach, including representatives of the Office of the Human Rights Commissioner with special responsibility for Child Rights, the Royal Malaysia Police Sexual, Women and Children Investigation (D11) Division, the Principal Assistant Director and the Director of the Anti-Human Trafficking and Migrants Smuggling Prevention Division.

The D11 division provides support services for children through victim care officers at Victim Care Centres. These victim care officers are all registered as counsellors and can assist in assessing a child before an investigation begins, and even provide multiple counselling sessions. (RA4-J-MY-09-A) An advisor to the Court of Children in Kuala Lumpur indicated that this was a crucial service because *"as police officers, we are facing difficulties in gaining confidence from the child victim first."* (RA4-J-MY-01-A)

In addition to counselling services, the D11 division was said to liaise with the Department of Social Welfare to obtain other necessary victim support services including shelter and foster-care services. (RA4-J-MY-09-A)

Despite the child-friendly measures implemented by law enforcement officers, and although it may not be common, it was suggested by one criminal justice professional (RA4-J-MY-05-A) that victim blaming by law enforcement officers still sometimes occurs during the interview process (see chapter 2.4.1).

Child Interview Centres

The law enforcement officials interviewed all agreed on the importance of child-friendly court proceedings and interviewing facilities and the use of recorded testimonies. They said that they had made use of laws such as the Sexual Offences against Children Act to secure resources and staff for law enforcement, including recording equipment. They also mentioned that non- governmental organisations played a significant role in facilitating interviews and providing psycho-social support and rehabilitation for the victims.

One especially promising practice in Malaysia is the use of Child Interview Centres. Criminal justice professionals interviewed for *Disrupting Harm* explained that there are Child Interview Centres in every state in Malaysia and that officers working with child victims often *"will not be in their official uniform"*, to ensure that the environment is child-friendly. (RA4-J-MY-09-A) The officers in these centres are specially trained to deal with child victims – something which is lacking in typical police stations, where interviews may resemble interrogations. (RA4-J-MY-05-A)

One criminal justice professional suggested that these centres should be introduced more widely across Malaysia. (RA4-J-MY-06-A) The same representative said that the centres had led to a great improvement in the way in which child victims were interviewed and helped to prevent the re-traumatisation of children going through the justice system. (RA4-J-MY-06-A) However, another criminal justice professional argued that the centres will only succeed if they are given proper funding and are staffed by adequately trained/skilled police officers. (RA4-J-MY-05-A)

Challenges regarding child interviews

Interviews with justice professionals revealed several concerns about the interviewing of children. One justice professional said that the police do not always use the Child Interview Centres or special rooms. (RA4-J-MY-06-A) The same respondent saw this as a problem because video-recorded evidence of children's interviews and statements are important for courts and should be obtained in the best possible environment for children. Two other representatives from NGOs agreed that there is a lack of uniformity in the interview process and called for all interviews to be standardised and consistently conducted in the Child Interview Centres. (RA4-J-MY-05-A, RA4-J-MY-07-A)

Justice professionals noted that interviews by insufficiently trained officers could lead to distress due to difficult/inappropriate lines of questioning or victim-blaming. (RA4-J-MY-05-A; RA4-J-MY-09-A) Several interviewees expressed concern about children having to undergo several interviews: *"When the child victims go for a medical examination, they will be interviewed by the Suspected Child Abuse and Neglect (SCAN) Team first, then by the police officers in the Child Interview Centre, and lastly, in the court by the Deputy Public Prosecutors and the defence lawyers"* (RA4-J-MY-10-A), and this was believed by justice professionals to result in greater trauma and suffering for child victims. (RA4-J-MY-10-A, RA4-J-MY-06-A, RA4-J-MY-03-A)

3.2.7 Passing the case on to the court

The government representatives interviewed for *Disrupting Harm* indicated that, in the three years since the enactment of the Sexual Offences against Children Act in 2017, few cases of OCSEA reported to the police had culminated in prosecution.

A few of the government representatives named specific obstacles, including the withdrawal of complaints by the children or their families, which can happen either at the investigation stage or after the prosecution has already been initiated (RA4-MY-10-A- justice), and out-of-court settlements in which the victim and offender settled outside the formal justice system. In the latter, the offender may provide financial compensation to the child, or the offender may marry the child to reduce the community stigmatisation of victims of sexual violence. (RA4-MY-10-A- justice)

Another obstacle mentioned in the interviews was a lack of sufficient digital evidence necessary to prosecute. (RA1-MY-01-A) For example, it was found that the Office of the Children's Commissioner had received one complaint that met the definition of child sexual abuse material under the Sexual Offences against Children Act and reported it to the police for investigation. However, the police took no further action because they had insufficient evidence to proceed.

In the cases investigated by the D11 division of the Royal Malaysia Police, the number of arrests has increased over the years, but this has not been matched by the number of prosecutions and convictions.

Figure 37: Outcomes of cases.

	2017	2018	2019
Arrests	5	8	13
Prosecutions	4	4	4
Convictions	0	2	1

Base: D11, Division of the Royal Malaysia Police.

The offenders in the cases investigated by the D11 division were variously charged under the Sexual Offences against Children Act,[147] the Child Act,[148] the Film Censorship Act[149] and Sections 377A, 377B, 377C, 372(1)(a) and 376(2)(d) of the Penal Code.[150] Sections 377A and 377B of the Penal Code criminalise homosexual acts. The cases presented below, although clearly being OCSEA-related crimes, were investigated under provisions criminalising homosexuality/intercourse against the order of nature.

> **In the cases investigated by D11, the number of arrests has increased over the years, however this has not been matched by the number of prosecutions and convictions.**

Case Study 3
Sports Coach

In 2017, a case was reported involving a 54-year-old school sports coach, who showed pornographic videos to two boys aged 14 and 15, both of whom were students at a secondary school. The coach allegedly also drugged the boys. After sexually assaulting the children, the offender bought them clothes, shoes, pants and even a mobile phone. One of the children lodged a complaint with the police. The case was investigated under Section 377A of the Penal Code of Malaysia. The suspect was charged with 19 counts of intercourse against the order of nature and outrages of modesty. The offender was not charged under the Sexual Offences against Children Act.

Case Study 4
High School Teacher

In 2018, a case was filed against a 41-year-old male teacher. The suspect is alleged to have first groomed the students by showing them pornographic videos. He then sexually assaulted the students aged 14 and 17 on the school premises. Following the abuse, the offender gave the victims a mobile phone, clothes and shoes. The case was lodged with police by one of the victims accompanied by two of his friends. The case was investigated under Section 377B of the Penal Code rather than the Sexual Offences Against Children Act. The suspect was charged with 19 counts of intercourse against the order of nature and outrages of modesty. The victims were referred to the social welfare department for follow-up, counselling and psychological support.

147. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017.
148. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001.
149. Government of Malaysia. (2002). Laws of Malaysia - Act 620 - Film Censorship Act.
150. Government of Malaysia. (1936). Laws of Malaysia - Act 574 - Penal Code, as amended in 2017.

3.3 OBTAINING JUSTICE AND ACCESS TO REMEDIES

3.3.1 Court proceedings

Capacity of criminal justice professionals

During the interviews with government representatives and criminal justice professionals, no mention was made of any structured and regular training for judges, prosecutors and lawyers in child-friendly approaches or about OCSEA. The interviewees emphasised the need for criminal justice professionals to receive adequate training on how to work with child victims and witnesses in court.

As regards the matter of whether OCSEA cases are handled by specialised professionals, respondents from law enforcement agencies explained that there are seven public prosecutors responsible for prosecuting online crimes against children under the Attorney General's Chambers. However, they did not indicate whether these prosecutors had received specialised training on the use of child-friendly approaches when interacting with child victims and child witnesses.

Child-friendly measures

The Evidence of Child Witnesses Act 2007 [Act 676] provides for a range of special measures to facilitate children's testimonies but it applies only to children under 16.[151] The act allows for a video-taped statement of the child's police interview to be used as evidence in chief.[152] Under Section 4, the act provides different ways to limit the contact between the child witness and the accused by placing a barrier between them or through the use of live or recorded videos.[153] As no victims of OCSEA were interviewed under *Disrupting Harm,* we cannot provide children's perspectives on how these special measures have been implemented in actual cases involving child witnesses.

According to government representatives, Malaysia established special courts to handle sexual crimes against children in 2017, but until now, only two special courts have been established: in Putrajaya and Kuching. The initiative has not yet been expanded to other states. The criminal justice professionals interviewed for *Disrupting Harm* reported that the special courts have child-friendly facilities such as private entrances and exits for child victims, child-friendly waiting rooms and video link facilities. Judges in these courts were also said to use child-friendly language. The justice professionals said that cases in these courts progress faster than in an ordinary court, except in cases in which multiple charges are laid.

According to the justice professionals, there are also some ordinary courts that handle child abuse cases sensitively. One interviewee gave the Kuala Lumpur Magistrate's Court as an example of a court in which child victims are handled with care and sensitivity and cases involving child victims are prioritised irrespective of the form of abuse involved. (RA4-MY-01-A- justice)

In ordinary courts, however, child-friendly waiting rooms and video link facilities are not always available. One respondent commented: *"Different [ordinary] courts have different facilities. For example, when we went to Melaka for a case, they had a children's room for child survivors and their families. However, in the Petaling Jaya courts or other courts in Klang Valley, only normal rooms are available for the child victims."* (RA4-MY-05-A- justice) A government respondent said that budget constraints have hindered the provision of child-friendly facilities as envisaged in the Evidence of the Child Witness Act. (RA1-MY-01-A) *"Allocation is not provided to expand the special court and [there is] no additional budget for it,"* confirmed another government representative. (RA1-MY-03-A&B)

151. Government of Malaysia. (2007). Laws of Malaysia - Act 676 - Evidence of Child Witness Act 2007, Section 2.
152. Government of Malaysia. (2007). Laws of Malaysia - Act 676 - Evidence of Child Witness Act 2007, Section 6.
153. Government of Malaysia. (2007). Laws of Malaysia - Act 676 - Evidence of Child Witness Act 2007, Section 4, paragraph 1.

In addition to the ordinary and special courts, Malaysia also has 'Courts for Children', which handle cases of children in need of care and protection and have the power to make orders in relation to the 'care and protection' of these children.[154] A child who has been sexually abused by a parent or guardian or a member of their extended family; or a child who has been sexually abused by another person, and a parent or guardian, knowing of such abuse, has not protected the child from such abuse, is considered a child in need of care and protection.[155]

Duration of trials

Chief Registrar Circular No. 2 Year 2017[156] states that criminal cases, including cases involving sexual offences against children, which are brought before lower courts must be concluded within 12 months. (RA1-MY-01-A) However, criminal justice professionals pointed out that criminal proceedings involving child victims of sexual abuse and exploitation can still be protracted. A representative of the Attorney General's Chambers commented: *"Some delays take roughly two years."* (RA4-MY-03-A- justice)

The main reason for such delays, in the words of one criminal justice professional, is that *"a lot of cases are handled by one Deputy Public Prosecutor [meaning each individual prosecutor has to handle a lot of cases]."* (RA4-MY-05-A-justice) Another justice professional concurred: *"The investigation officers have so many cases."* (RA4-MY-01-A-justice) A third criminal justice professional attributed the delay to the documentation process: *"The main reason for such a delay is mainly because of the documentation... It takes about six months to complete the documentation and paperwork process."* (RA4-MY-03-A- justice)

According to another criminal justice professional: *"The child victims frequently have a difficult time recalling their traumatic incidence [when giving testimony in court] because it happened two or three years ago."* (RA4-MY-04-A- justice) This might be an indication that the quality and chance of a successful prosecution decrease the longer a case is delayed.

Legal aid

In 2017, amendments to the Legal Aid Act of 1971 [Act 26][157] introduced legal companion services for child victims of sexual assault. (RA4-MY-08-A-justice) The purpose of a legal companion is to provide legal advice to the guardian or protector of the child victim, to obtain relevant legal information relating to any criminal proceedings to which the victim is a party, to accompany the victim in any court proceedings, and, with permission of the court, to speak on behalf of the victim.[158] An application, however, has to be made by the victim in order to access this service.[159]

Interviews with criminal justice professionals revealed that the uptake of the legal companion's service is low. A criminal justice professional representing the Attorney General's Chambers stated: *"I am aware of the legal companion services. However, in my experience, I have never come across any legal companion services provided by the Legal Aid Department."* (RA4-MY-03-A- justice) The low uptake was attributed to insufficient promotion of the service by the Department of Legal Aid under the Legal Affairs Division of the Prime Minister's Department.

Aside from the legal companion services provided by the Department of Legal Aid, the Malaysian Bar Council was also said by one criminal justice professional to provide legal assistance services. (RA4-MY-02-A- justice)

3.3.2 Compensation

In Malaysia, child victims of OCSEA can seek compensation in criminal proceedings from convicted offenders. Section 426 (4) of the Criminal Procedure Code also entitles them to initiate an independent civil suit for the recovery of any property or the recovery of damages beyond the amount of compensation paid under an order given in a criminal proceeding.[160]

154. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001, as amended in 2017, Part V.
155. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001, as amended in 2017, Section 17 (1) (a) and (b).
156. Pekeliling Ketua Pendaftar Bilangan 2 Tahun 2017.
157. Government of Malaysia. (1971). Laws of Malaysia – Act 26 - Legal Aid Act 1971, as amended in 2017.
158. Government of Malaysia. (1971). Laws of Malaysia – Act 26 - Legal Aid Act 1971, as amended in 2017, Section 29I.
159. Government of Malaysia. (1971). Laws of Malaysia – Act 26 - Legal Aid Act 1971, as amended in 2017, Section 2A.
160. [1] Government of Malaysia. (1935). Laws of Malaysia – Act 593 - Criminal Procedure Code, as amended in 2012, Section 426 (4).

Challenges regarding compensation

According to the criminal justice professionals interviewed, deputy public prosecutors are responsible for submitting applications for compensation to the court on behalf of victims, but they do not always do so. According to one criminal justice professional: *"If the Deputy Public Prosecutor does not seek compensation, then the court has no power to grant any compensation."* (RA4-MY-10-A- justice)

A criminal justice professional from the Attorney General's Chambers indicated that there are currently no specific guidelines for determining the amount of compensation to be sought and emphasised the need to amend the Criminal Procedure Code in order *"to provide more details for determining the quantum of the compensation and introduce guidelines for the deputy public prosecutors who handle child abuse cases on the procedures to apply for compensation in court."* (RA4-MY-03-A-justice)

It was also reported that *"many child victims and their families are not aware of the compensation provisions provided for the child victims."* (RA4-MY-05-A-justice) The reason as to why there are few applications could be that victims are unaware of their rights and do not, therefore, put pressure on deputy public prosecutors to apply for compensation.

Two interviewees from the Attorney General's Chambers (RA4-MY-03-A- justice; RA4-MY-04-A- justice) also expressed concerns about the enforcement of compensation orders awarded by the courts. On the basis of their past experience, they stated that many convicted offenders do not have the financial capacity to pay compensation. When a convicted offender defaults on compensation payments, the length of his/her prison sentence is increased.

3.3.3 Social support services for children

Where services are provided

According to the interviews with criminal justice professionals, the support services available to child victims of abuse including OCSEA include shelter where it is needed, medical services and counselling/psycho-social support.

The **Department of Social Welfare** provides shelter for victims of neglect, abuse, abandonment and exploitation. (RA4-MY-04- A- justice) While children are best protected in a home environment, rescue or temporary shelter services are needed if the situation at home is unsafe or alternative family-based care is not immediately available. If shelters are utilised, their operation must comply with appropriate international standards, such as the UN Guidelines for the Alternative Care of Children.[161]

With respect to counselling services, a respondent from the special court for Sexual Crimes against Children stated that no counsellors from the Department of Social Welfare attend the court with child victims. The respondent attributed this to the lack of counsellors at the Department of Social Welfare. (RA4-MY-10-A- justice)

One-Stop Crisis Centre services have been designed to provide immediate medical treatment and psychological support to adult (and sometimes child) survivors of abuse, domestic violence, rape and sexual abuse in collaboration with other agencies. This service is present in all major government hospitals. However, they are not always actual physical spaces as initially planned (incorporating an interview room, specialised examination room, family room, etc.). The One-Stop Crisis Centres have a relatively formal staff structure, but they are not officially hospital units or departments.[162]

161. UN General Assembly. (2010). Resolution adopted by the General Assembly [on the report of the Third Committee (A/64/434)] 64/142. Guidelines for the Alternative Care of Children.
162. Child Frontiers and the Malaysian Association of Social Workers (2022). Mapping and Assessment of the Social Service Workforce in Malaysia. UNICEF.

One-Stop Crisis Centres conduct an initial medical examination provided that the condition of the child is not critical. If the child is in a critical or semi-critical condition, he/she is referred to an emergency unit.[163] One criminal justice professional interviewed by *Disrupting Harm* stated that medical services for child sexual abuse cases that are provided by the One-Stop Crisis Centres are very effective. (RA4-MY-05-A-justice) It was not clear from the interviews how many One-Stop Crisis Centres have been established.

The Suspected Child Abuse and Neglect (SCAN) team is a well-recognised 'mechanism' within the One-Stop Crisis Centres with the role of specifically managing children's cases. It falls under the charge of a senior paediatrician. The SCAN teams are a multi-disciplinary group of professionals from various medical and social fields, but include paediatricians, medical social workers and counsellors, among others, who have been trained to recognise and appropriately manage cases of child abuse. A representative from the Department of Social Welfare is represented on the team, and they work closely with the Royal Malaysian Police, representatives from the Ministry of Education, the State Islamic Department (*Jabatan Islam Negeri*), the Government's Legal Aid Bureau, the National Registration Department and other relevant agencies. In practice, the composition of the SCAN teams depends upon resources and is not strictly uniform across hospitals, although an entire team is generally in place at all government hospitals. There is, however, strict guidance for referral to a 'higher-level hospital' when faced with severe cases and the service of certain medical professionals is not available. Nevertheless, all SCAN teams work according to similar guidelines.[164]

The **Special Prosecution Unit** under the Prosecution Division of the Attorney General's Chambers has a psychologist to assist child victims before and during trials.

Non-governmental organisations offer comprehensive victim support services in collaboration with the government, according to the interviews with criminal justice professionals (see chapter 3.5.1 for more information).

As described in chapter 3.2.6, the **D11 police unit** provides support services for children through care officers at Victim Care Centres.

Challenges regarding support services

A lack of clear referral pathways to One-Stop Crisis Centres: A Ministry of Health official interviewed for *Disrupting Harm* reported: *"There is no clear referral pathway from district clinics or community clinics to the hospitals where the One-Stop Crisis Centre is located."* (RA1-MY-05-A) The official added, however, that the Ministry is drafting a training module for frontline health staff in all community health clinics concerning the procedures to be followed for the early detection of sexual abuse cases, and that the module encompasses ways of referring such cases to the One-Stop Crisis Centres in hospitals. Moreover, the Ministry of Health is drafting training modules for teachers that focus on detecting signs of abuse in schools, and these modules also explain the referral pathway to the One-Stop Crisis Centres in hospitals. (RA1-MY-05-A)

Inconsistencies in the medical services provided: One criminal justice professional said that there are inconsistencies in the provision of medical services due to differences in the practices of frontline workers in hospitals, especially in rural areas. (RA4-MY-07-B- justice) A respondent from the Ministry of Health pointed out that there are no clear standard operating procedures. (RA1-MY-05-A)

Uneven distribution of services: Among the 50 frontline workers surveyed, 42 agreed that the concentration of services in urban areas affected the availability of support services for children recovering from OCSEA. This was the most important obstacle to access to these services, according to the survey.

163. Ministry of Health Malaysia. (2009, June 12), Guidelines for the hospital management of child abuse and neglect. MOH/P/PAK/130.07 (GU). Medical Development Division, Ministry of Health Malaysia, 16–18.
164. Child Frontiers and the Malaysian Association of Social Workers (2022). Mapping and Assessment of the Social Service Workforce in Malaysia. UNICEF.

3.4 POLICY AND GOVERNMENTAL RESPONSE TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

3.4.1 Policy and governance

Responsible agencies

The government agencies in Malaysia with a mandate to address OCSEA are as follows:

- The Ministry of Women, Family and Community Development – The ministry is in charge of child protection policies in Malaysia and operates the Talian Kasih 15999 hotline.
- The Department of Social Welfare of Malaysia – This department provides care and rehabilitation to vulnerable groups, including children.[165] This agency also has the mandate of employing the staff who manage social welfare services for the most vulnerable populations and is responsible for ensuring high-quality service delivery.
- The Malaysian Communications and Multimedia Commission[166] – The commission assists the Royal Malaysia Police by blocking access to websites containing child sexual abuse materials and also helps with suspect identification and digital forensic analysis.[167] The commission also implements Internet Centres across the country with support from Telecommunication companies.
- CyberSecurity Malaysia – This agency addresses computer security concerns and combats cyberattacks through MyCERT. Their Computer Emergency Response Team operates the Cyber999 Help Centre, which allows internet users to report online incidents.
- The Ministry of Science, Technology and Innovation – The ministry is responsible for developing ICT initiatives and providing funding for technology development and innovation.
- The Ministry of Education[168] – The ministry contributed to the Plan of Action on Online Child Protection 2015–2020 and contributed to the implementation of the CyberSAFE in Schools programme with CyberSecurity Malaysia.
- The Royal Malaysia police.
- The Attorney General Chambers.
- The National Cyber Security Agency – The agency launched the Malaysia Cyber Security Strategy 2020–2024 and, according to the government representatives (RA1-MY-09-A, B & C) interviewed, will be taking steps to enhance the capacity and capability of law enforcement agencies to tackle cybercrime by developing and implementing a new National CyberCrime Enforcement Plan. Under this forthcoming plan, efforts will be made to increase the knowledge and skill of judiciary members, prosecutors, law enforcement officers and legal practitioners as regards preparing them for the intricacies of cybercrimes in the digital era.

In addition to the above, the following ministries are important: The Ministry of Health, as the health system plays a vital role as the gateway to identification and support for victims, and the Ministry of Finance, as budget allocation to mandated government agencies for the implementation of OCSEA-related programmes is a crucial part of the national response to OCSEA.

Government initiatives to address OCSEA

Representatives of the various government institutions described several efforts made by government agencies in collaboration with non-governmental entities to create public awareness and spread information concerning child sexual abuse and exploitation.

National programmes: National-level awareness initiatives that discuss internet safety undertaken by the government in collaboration with other partners include:

CyberSAFE[169]

Launched in 2009, the Cyber Security Awareness for Everyone (CyberSAFE) initiative was led by Cybersecurity Malaysia. It aimed to increase public awareness and knowledge about cyber safety and how to mitigate online risks.[170] It provided cyber tips, games, quizzes, videos, posters and tools for children, youth, parents, organisations and communities.

165. African Union Commission (11–12 December 2019). Speech by YB Ms. Hannah Yeoh, Minister of Women, Family and Community Development, Malaysia.
166. Malaysian Communications and Multimedia Commission.
167. Pemberitahuan Pertanyaan Lisan Dewan Negara Mesyuarat Ketiga 2019, Penggal Kedua Parlimen Keempat Belas.
168. Kementerian Pendidikan Malaysia.
169. CyberSAFE Malaysia.
170. CyberSAFE Malaysia.

The CyberSAFE in Schools programme, which was a part of the CyberSAFE initiative, was undertaken in partnership with Cybersecurity Malaysia, the DiGi, Childline Malaysia, the Malaysian Communications and Multimedia Commission and the Ministry of Education. Its goal was to reach out to school children via outreach programmes and CyberSAFE ambassadors and to provide teacher training workshops. As of 2015, it had engaged with more than 100,000 school children in more than 1,400 schools nationwide.[171] The programme produced books and videos that show how to deal with cyberbullying, cyberstalking and grooming. Through the website, children could learn about cybersafety through contests, games and videos. CyberSAFE conducted an annual CyberSAFE in Schools National Survey to evaluate the scope of online risks and harm to children.[172]

Klik Dengan Bijak (KDB) ("Click Wisely")
In 2012, the Malaysian Communications and Multimedia Commission worked with a range of stakeholders to introduce the "Klik Dengan Bijak (KDB)/Click Wisely" education and awareness-raising programme on safe and responsible use of the internet. The programme was mainly directed towards children and youths, but also targeted parents and other caregivers. It aimed to "generate literate users of technology and new media content, educate internet users about the importance of self-regulation, create a sense of responsibility among internet users and a safe environment for internet users".[173] The programme was supported by the Ministry of Education, Science, Innovation and Technology, the Ministry of Youth and Sports, the Royal Malaysia Police, the National Service Training Department and the Communications and Multimedia Content Forum of Malaysia.

National Cyber Security Awareness Module
The National Cyber Security Awareness Module, which involves CyberSecurity Malaysia, was described by two government representatives as a nationwide educational initiative that addresses cybercrime (including OCSEA) in the classroom. (RA1-MY-09-A, B &C)

Other initiatives:

The development of risk mitigating/parental control tools
A representative from the Malaysian Communications and Multimedia Commission reported that the Commission has *"asked the Internet service providers to have parental control tools available for their subscribers."* This informant added that, although *"risk mitigating tools"* are available, *"the take up is very little"* because parents are unaware of them. (RA1-MY-02-A &B)

Safe and unsafe touch programme
The Ministry of Women, Family and Community Development launched five videos on YouTube in collaboration with Google Malaysia to spread the message about Safe and Unsafe Touch as part of sexual education for parents and children.[174] Two government representatives interviewed by *Disrupting Harm* (RA1-MY-03-A&B) referred to the 'Safe and Unsafe Touch' programme as a successful case of collaboration to raise awareness about CSEA.[175] It was unclear, however, whether any information directly related to OCSEA was included.

Digital parenting and child online protection forum
In June 2019, the National Population and Family Development Board, in collaboration with UNICEF and other government partners concerned with child wellbeing, came together at a forum to discuss digital parenting for better child online protection. The forum aimed to guide the development of a new training module on Digital Parenting and Child Online Protection for the Semarak Kasih Parenting Programme. The National Population and Family Development Board, in partnership with University Putra Malaysia, Maestral International and UNICEF, revised and strengthened a number of training modules to guide parenting support interventions.[176]

171. DiGi Telecommunications. (2015). The National Survey Report 2015. Growing Digital Resilience among Malaysian Schoolchildren on Staying Safe Online Presentation.
172. UNICEF (2016). Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.
173. Malaysian Communication and Multimedia Commission. (2012 July 6). "Klik Dengan Bijak" Campaign.
174. African Union Commission (11–12 December 2019). Speech by YB Ms. Hannah Yeoh, Minister of Women, Family and Community Development, Malaysia.
175. Women, Family and Community Development Ministry of Malaysia. (2019, July 13). Safe and Unsafe Touch [Video]. YouTube.
176. UNICEF Malaysia. (2019 June 20). Parents determine child's early experience online; Better parenting means a safer internet for children [press release].

For example, the Naungan Kasih sexual and reproductive health module covers the following topics: sexual and reproductive child rights, sexuality, and parents' role in sexuality education, puberty, safe and unsafe touch, intimate relationships, sexual consent, child marriage and disclosure of sexual abuse.

Other awareness-raising initiatives on child online protection mentioned by the government representatives interviewed include the PEKA and PEKERTI programmes and Cybersafe Parenting-Towards Cyber Wellness. (RA1-MY-09-A, B &C; RA1-MY-09-A, B &C) The fact that some of these programmes and educational materials are targeted at caregivers, and not only at children, indicates the emphasis which Malaysia wishes to place on caregivers when addressing child online safety. It is not clear how much focus is given to OCSEA in these programmes.

Effectiveness of awareness-raising efforts

The interviews with government representatives and justice professionals revealed that awareness-raising efforts are perceived to have resulted in an increase in the reporting of CSEA offences. (RA1-MY-07-A; RA4-J-MY-09-A) However, it was also noted that there is insufficient monitoring and evaluation of current public awareness efforts (RA1-MY-07-A; RA4-J-MY-01-A), particularly with respect to OCSEA. It is, therefore, not known how much knowledge has been retained by the target groups. The receptiveness of the public to such initiatives is also open to question. Both the frontline workers survey and interviews with justice professionals confirmed the perception that cultural discomfort discussing sex and sexuality has stunted efforts to increase awareness of OCSEA in the public. (RA3-MY-13-A; RA3-MY-38-A; RA4-J-MY-02-A)

3.4.2 Challenges to the governmental response to OCSEA

Capacity constraints: The government representatives interviewed highlighted staff shortages at the government agencies with mandates related to OCSEA. According to one individual, the unit for children under the Ministry of Women, Family and Community Development has a limited number of personnel dedicated to children's issues. (RA1-MY-03-A&B)

Another interviewee reported that child protectors working for the Department of Social Welfare have to handle at least 80 children's cases at any given time. This respondent said that the shortage of social workers was a longstanding issue. (RA1-MY-07-A&B) Though the Department of Social Welfare, through the Welfare Training Institute, builds the capacity of qualified social workers joining the Ministry of Social Welfare and provides in-service training on child protection for Ministry of Social Welfare staff,[177] one government representative noted that the training provided by the Department of Social Welfare for both newly appointed and existing protectors every year, is not consistent. (RA1-MY-07-A&B)

Budget: Almost all the participants in the research confirmed that there was no specific budget for OCSEA and that *"more resources need to be allocated"*. (RA1-MY-03-A&B) In this context, a government representative suggested that greater priority needs to be given for social development in tandem with a focus on promoting economic growth. (RA1-MY-03-A&B) Giving the example of the Sahabat BIJAK: Safe and Protect programme, another respondent stated that only 4% of the 10,202 schools in Malaysia have implemented the programme due to a decrease in the financial resources allocated by the government. (RA1-MY-07-A)

Coordination: The government representatives interviewed pointed out that there are gaps in the way mandated government agencies communicate and share data with each other: *"The government agencies do not communicate inter-agency well and do not work together by sharing crucial data in hopes to aid the investigation."* (RA4-MY-01-A- justice) Although a Child Online Protection Taskforce was established in August 2013, for the purpose of drafting the Plan of Action on Child Online Protection, which lapsed in 2020, at the time of data collection, the taskforce appeared to no longer be active.[178]

177. Child Frontiers and the Malaysian Association of Social Workers (2022). Mapping and Assessment of the Social Service Workforce in Malaysia. UNICEF.
178. Internet Society. (2017). Mapping Online Child Safety in Asia Pacific.

3.5 COORDINATION AND COLLABORATION WITH NON-GOVERNMENT ENTITIES

3.5.1 Civil society

The criminal justice professionals interviewed said that non-governmental organisations, such as Protect and Save the Children, the Women's Aid Organisation and the Women's Centre for Change, offer comprehensive victim support services in collaboration with the government. The Women's Aid Organisation was said to offer *"help during the investigation and assist the child victims with court proceeding stages including preparation of the child victim impact statements"* (RA4-MY-05-A- justice), while Protect and Save the Children case managers were reported to *"accompany the child victim and attend the court proceedings."* (RA4-MY-07-A- justice) Aside from victim support, civil society organisations in Malaysia also collaborate with the government on awareness-raising initiatives.

3.5.2 Internet service providers and platforms

Domestic Internet service providers

The communications and technology industry in Malaysia has shown a promising level of engagement in combating OCSEA.

Evidence gathering: Malaysia has not established a legal obligation for Internet service providers to report websites on which sexual abuse materials representing children are available. However, the Communications and Multimedia Act, enacted in 1998, states that Internet service providers are criminally liable if they provide content that is indecent, obscene or offensive in character with the intent to annoy, abuse, threaten or harass.[179] According to the Malaysian Communications and Multimedia Content Code issued in 2004, "child pornography" is included within the category of prohibited obscene content.[180]

The Evidence Act establishes the presumption that owners, hosts, administrators, editors, sub-editors and subscribers of network service providers have published all content that appears under their name, using their photograph or pseudonym.[181] Consequently, website hosts, forum administrators and even social media platforms could be held accountable for the publication of materials depicting sexual abuse of children. This provision of the act is seen as a potential tool for preventing and combating the circulation of CSAM. However, it has also been the subject of protests online due to limitations on freedom of expression.[182]

Interviews with government representatives revealed that, even though Internet service providers are not legally required to report and work with law enforcement, they often comply with requests if they have stored the information. Interviews with law enforcement officers also revealed that there is a system in place to retrieve data from Internet service providers and social media service providers. However, no further information was provided as to how this system operates, how it ensures/encourages compliance and whether it includes timelines for compliance. A representative of DiGi Telecommunications, which is also an Internet service provider, confirmed that the company discloses data to law enforcement agencies for OCSEA investigations.

Even though Internet service providers are willing to cooperate with law enforcement agencies, a representative of the Sexual, Women and Child Investigations Division (D11) of the Royal Malaysia Police stated: *"The effort to identify users is often hampered due to the lack of a mandatory data retention/preservation law in the country."* (RA1-MY-11-A)

179. Government of Malaysia (1998). Laws of Malaysia - Act 588 - Communications and Multimedia Act 1998, Section 211.
[1] Communications and Multimedia Content Forum of Malaysia (CMCF). (2004). The Malaysian Communications and Multimedia Content Code, Part 2 (3).
180. Communications and Multimedia Content Forum of Malaysia (CMCF). (2004). The Malaysian Communications and Multimedia Content Code, Part 2 (3).
181. Government of Malaysia. (1950), Laws of Malaysia – Act 56 - Evidence Act 1950, as amended in 2017, Section 114A.
182. Centre for Independent Journalism. (n.d.), Stop 114A, 14 August 2012 Internet Blackout page.

Another government representative confirmed this: *"What we practice now is once we received the information from counterparts, we want to identify the suspect or subscriber. Sometimes, they [internet service providers] have no more information available since there is no standard period to keep the data. DiGi and TM [Telekom Malaysia] have an internal policy to maintain the data of the subscribers for at least a month. So, this is what we are facing when we want to request details about the subscriber based on what time he accesses these IP addresses. This is the problem because we are dealing with IP address identification of the perpetrator or offender."* (RA1-MY-02-A &B)

Removing/reporting CSAM: The Malaysian Communications and Multimedia Commission is responsible for prohibiting offensive content and assists the Royal Malaysia Police by blocking access to websites containing child sexual abuse materials and with suspect identification and digital forensic analysis. There is no legal obligation for Internet service providers to remove or block access to websites on which sexual abuse materials representing children are available.[183] Despite the lack of a legal obligation, a representative from DiGi told *Disrupting Harm* that the company has been using INTERPOL's Worst Of URL List since 2013 to block access to known CSAM URLs as part of a wider initiative from its shareholder Telenor.

Awareness raising: The domestic Internet service provider DiGi Telecommunications has been involved in awareness raising regarding internet safety at the grassroots level, especially through programmes in schools. This focused on topics such as online dating, sexual violence and how to report abuse. As mentioned in chapter 3.4.1, DiGi has been involved in the Cybersafe programme in schools, which it implemented in collaboration with mandated government agencies. The partnership between the government and DiGi in the Cybersafe In Schools programme is a good example of how the public and private sectors can work together to promote a common interest.[184]

Global platforms

Evidence gathering: Global platforms cannot be compelled to disclose information by Malaysian court orders or Malaysian authorities since they are governed by the domestic laws in their own countries. In the case of the United States, the Stored Communications Act and Electronic Communication Privacy Act. U.S. Law expressly prohibits the disclosure of communications content such as messages and images directly to non-U.S. law enforcement authorities. However, U.S.-based tech platforms may voluntarily disclose non-content data to foreign authorities, including subscriber data and IP logs needed for conducting investigations.

A representative from DiGi reported that, while the big U.S. platforms are very responsible in their approach, children in Malaysia often use Korean, Chinese or Indonesian apps, and the Malaysian authorities have very limited dialogue with these companies with regard to OCSEA.

Removing/reporting CSAM: With respect to removing/reporting CSAM, there are rarely any formal agreements between national law enforcement agencies and global platforms. The platforms would prefer to view requests from government partners as notifications of potential violations of their own terms of service. Since CSAM is contrary to the platforms' terms of service and U.S. law, it would be in the companies' interests to remove such content.

183. Internet Society (2017). Mapping Online Child Safety in Asia Pacific. Singapore: Internet Society APAC Bureau.
184. UNESCO Bangkok (2016). A Policy Review: Building Digital Citizenship in Asia-Pacific through Safe, Effective and Responsible Use of ICT.

Transparency Data[185]

In 2017, 2018 and 2019, the transparency reports of major social media platforms show that authorities in Malaysia made:

- 285 requests to Facebook for content restriction, for reasons including blasphemy, hate speech, privacy violation, the spread of false information, the promotion of regulated goods, private cases of defamation and illegal bullying (four items, H2 2018);
- 180 requests for Facebook user data;
- 214 requests to Google for content removal, of which 19 concerned adult content, 42 bullying/harassment and 11 obscenity/nudity;
- 9 requests for Google user data;
- 13 requests to Apple;
- 7 requests to Twitter for user data, and 73 for content removal;
- 8 requests to Tumblr for content removal;
- 24 content removal requests and 2 user data requests to Verizon Media.

While the types of crime in connection with which the majority of these requests were made cannot be identified from the available data, the diversity of platforms addressed indicates a certain level of engagement with U.S. technology companies.

185. The annual transparency reports of major social media platforms provide statistics on the number of requests for user data and content removal from each country's government authorities. Platforms were selected on the bases of high volumes of reports to NCMEC (10,000+), availability of transparency reporting and known popularity in *Disrupting Harm* focus countries. In addition to U.S.-based companies, transparency reports for Line and TikTok were also reviewed. Data was extracted from corporate websites on 13/08/2020, 18/08/2020 and 04/12/2020. Companies publish their reports in various formats. This required a certain amount of manual data cleaning and reviewing. Every effort was made to check the accuracy of the datasets subjected to manual manipulation.

4. HOW TO DISRUPT HARM IN MALAYSIA

Disrupting harm from online child sexual exploitation and abuse requires comprehensive and sustained action from all stakeholders – families, communities, government representatives, law enforcement agencies, justice and social support service professionals and the national and international technology and communications industry. While children are part of the solution, the harm caused by OCSEA obliges adults to act to protect them; we must be careful not to put the onus on children to protect themselves from harm without support.

The following detailed recommendations for action in Malaysia are clustered under six key insights from the *Disrupting Harm* data and are signposted for different stakeholder groups. However, all these recommended actions are interlinked and are most effective if implemented in coordination.

4.1 SIX KEY INSIGHTS AND RECOMMENDATIONS FOR ACTIONS

Disrupting Harm Alignment with the Model National Response

Many countries, companies and organisations have joined the WePROTECT Global Alliance to prevent and respond to online child sexual exploitation and abuse. Despite not being a member of the Global Alliance, Malaysia can use the Model National Response to Preventing and Tackling Child Sexual Exploitation and Abuse to help organise its response to OCSEA. The model is a valuable tool for governments to improve the level of their response.

The majority of the recommendations in this report align with the 21 'capabilities' articulated in the Model National Response. Most *Disrupting Harm* recommendations address legislation,[186] dedicated law enforcement,[187] judiciary and prosecutors[188] and education programmes.[189]

However, *Disrupting Harm* identifies priority areas for interventions based specifically on the data gathered in Malaysia.

ASEAN recently endorsed the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN.[190] This Action Plan includes commitments for member states to strengthen online child protection in the region. The plan has seven focus areas ranging from awareness raising and strengthening data collection to legislative reform. The actions recommended by *Disrupting Harm* constitute sustained, practical and evidence-based activities that can be implemented in Malaysia as part of its commitment to the Regional Plan of Action.

INSIGHT 1

In the past year, at least 4% of internet-using children aged 12–17 in Malaysia were subjected to clear instances of online sexual exploitation and abuse that included being blackmailed to engage in sexual activities, someone else sharing their sexual images without permission, or being coerced to engage in sexual activities through promises of money or gifts. Scaled to the population, this represents an estimated 100,000 children who may have been subjected to any of these harms in a single year.

Government

1.1 Continue to engage the public – including children, caregivers, teachers and others – in awareness of violence against children including OCSEA via existing national programmes.[191] **Ensure that:**

- Awareness and education programmes are evidence-based. They should be developed and tested through safe and ethical consultations with children,[192] caregivers and teachers to ensure that they address their lived experiences of online risks and also include the techniques children use to keep themselves safe. This will help to create campaign messages that are relevant to children and are, therefore, more likely to resonate with them.

186. Model National Response #3.
187. Model National Response #4.
188. Model National Response #5.
189. Model National Response #13.
190. ASEAN. (2019). Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN.
191. This aligns with the ASEAN Regional Plan of Action Activity 6.2.1 on supporting mass and targeted public campaigns on online safety. ASEAN. Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN: Supplement to the ASEAN Regional Plan of Action on the Elimination of Violence Against Children. (forthcoming).
192. In Malaysia, the Children's Representative Council (MPKK) under the Ministry of Women's Children's Division could be engaged. The representatives comprise of 30 adolescents aged 13–17 years old from across each state in Malaysia. MPKK is the official children's consultative mechanism, and two representatives from MPKK are members on the National Children's Consultation Council mandated under the Child Act to promote the involvement of children in decision-making processes.

- Existing evidence-based programmes that have proven to be effective are adapted and contextualised to Malaysia and are prioritised and sustained.
- The campaigns have universal reach. Children aged 12–13 and children living in rural areas were found to be the least likely to have received information on how to stay safe online. Out-of-school children must also be reached.
- Interventions and programmes are monitored and evaluated, and use is made of innovative tools such as the online safety programmes evaluation model,[193] which was recently developed by a global panel of experts on online safety. This framework of indicators was designed to address the specific challenges of the East Asia and Pacific regions.

Awareness programmes should:

- Make children, caregivers and teachers fully aware of the role technology might play in the sexual exploitation and abuse of children.
- Equip adults and children to recognise signs of potential abuse and inform them about how and where to seek help for oneself or for others.
- Target boys and girls equally, as in Malaysia, it is equally common for boys and girls to be subjected to OCSEA.
- Equip caregivers with the knowledge and skills to foster safe and ongoing communication with children about their lives – both online and offline – leveraging, when possible, existing positive parenting programmes in Malaysia.
- Support caregivers – especially older caregivers who are infrequent users of the internet – in communicating with children about their lives online and in becoming more familiar with the platforms that children are using. Best practices already exist[194] and can be built upon and set in the local context.
- Foster an environment in which children are more comfortable having conversations about sexuality or asking adults, including teachers, for advice. Feelings of discomfort, shame or embarrassment can make children reluctant to discuss sexuality with adults; in fact, up to 22% of the children surveyed said they *did not want* to receive any sex education, which may indicate that children perceive discussing sexuality as stigmatising. While children should not be forced to engage in conversations that they are not comfortable with, in the context of OCSEA, it would be beneficial if adults create an environment in which children feel safe enough to report and seek help when experiencing sexual exploitation or abuse.
- Emphasise that child abuse and exploitation, in any form, should never be tolerated and that an experience of abuse or exploitation is never the child's fault.

These messages should be disseminated via the channels preferred by the recipients:

- The *Disrupting Harm* data shows that school teachers are both the primary source and a preferred source of age-appropriate comprehensive sexuality education and information for children. They are also one of the possible points of disclosure for a proportion of children. Engaging teachers in campaigns is critical, not only for disseminating key messages, but also for building trust and a sense of safety so as to enhance the opportunity for an open conversation and, where necessary, disclosure.

193. UNICEF (forthcoming). Evaluating Online Safety: What Works to Keep Children Safe Online.
194. See the Australian eSafety Commissioner's programme 'Start the Chat' to encourage caregivers to talk with their children about their lives online; and eSafety Commissioner's programme for seniors going online for the first time 'Be Connected'.

- For caregivers, the *Disrupting Harm* survey highlighted family or friends, social media, television and children's schools as actual and preferred channels for receiving guidance on children's internet use and how to keep them safe. Parenting online apps may also be a useful channel in Malaysia. One in five of the caregivers surveyed also received information from religious leaders. Taking into account caregivers' individual characteristics and preferences, these channels could be leveraged to disseminate awareness-raising messages or educational programmes about how caregivers can empower children to use the internet safely and effectively.

The government body suggested to lead in implementing this recommendation is the Ministry of Women, Family and Community Development, with the support of Ministry of Health, Ministry of Education, Ministry of Youth and Sports and the Ministry of Communication and Multimedia.[195]

1.2 Invest in digital literacy programmes for children, caregivers and teachers

- Provide comprehensive digital literacy and safety training to ensure that children and trusted adults are both aware of possible risks and know what to do about them. This should include information about what children can do if they are being bothered online, what kind of content is appropriate to share online with others and basic skills such as how to change their privacy settings and block people from contacting them. Thirty-seven percent of the children surveyed had never received information on how to stay safe online.
- Integrate cybersafety education into national school curricula and empower teachers to guide children's internet use. Existing programmes[196] in Malaysia should be evaluated and expanded.
- Ensure that these programmes reach younger children and children in rural areas, who have the lowest rates of risk awareness and digital skills, and children not in school.
- These programmes should consider the specific challenges faced by marginalised groups of children and their caregivers and the needs of children with low literacy levels.
- Integrate digital literacy information into positive parenting programmes.[197] Youth-led and youth-serving organisations could also be engaged to deliver digital training.[198]

1.3 Increase coordination and cooperation across programmes focused on online and offline violence and, to the extent that it makes sense, with programmes focusing on violence against women and children.

Caregivers, teachers and social support services[199]

1.4 Engage with children about their online habits and activities and teach them about the potential risks that exist online, possible protective measures and what to do if they encounter harm online. Overall, caregivers in Malaysia are likely to be familiar with the digital environment and have strong digital skills. They can make use of this knowledge to keep up to date with their children's online experiences. Older caregivers tend to have a much lower level of digital skills and are much less likely to engage in online activities. They, therefore, require tailored programmes that focus on parenting skills, such as how to engage in meaningful enabling mediation, and encompass basic online safety skills, including the nature of online risks and how they may lead to harm.

195. The recommendations for the leading organisations and bodies are based on discussions with over 98 participants – from government, law enforcement, CSOs and NGOS – at the national consultation for the *Disrupting Harm in Malaysia* report.
196. Examples include Yellow Heart by DiGi and DiGi CYBERSAFE (Education Ministry, CyberSecurity Malaysia, Childline Malaysia, Malaysian Communications and Multimedia Commission and DiGi).
197. Existing initiatives in Malaysia could be leveraged. UNICEF MY/National Population and Family Development Board (LPPKN), parents and other government partners came together at a forum to discuss digital parenting for better child online protection. Under the guidance of the forum, a new training module on Digital Parenting and Child Online Protection was developed for the Semarak Kasih Parenting Programme. This module focuses on how to establish rules and guidelines for appropriate digital device use by adolescents, creating a family media plan on safety, establishing privacy controls, monitoring online use, engaging adolescents in discussions about personal privacy and responding to OCSEA instances when they arise. The module will be delivered along other parenting modules, as part of a coherent intervention.
198. Such organisations include Monsters Among Us, WOMEN-girls, KRYSS Network.
199. Government, intergovernmental agencies and civil society need to translate and convey these messages to reach caregivers, teachers and social support staff.

INSIGHT 2

According to the household survey, while offenders of OCSEA are often someone unknown to the child, in some cases offenders are individuals the child already knows – often an adult acquaintance, a peer under 18 or a family member.

Government

2.1 Implement programmes that cover sexuality education. Sixty percent of the children surveyed in Malaysia had not received any sex education.

- Programmes should cover issues such as consent, personal boundaries, what adults or others around children can and cannot do to them, risks and responsibilities when taking, sending and receiving sexual images, and how to say 'No' to others. Comprehensive sexuality education should cover OCSEA and how technology plays a role in the sexual abuse and exploitation of children and equip children to recognise inappropriate interactions both online and offline. Programmes should be age-appropriate, gender-sensitive and provide accurate information. Programmes should be monitored and evaluated by child protection experts. While some initiatives already exist in Malaysia,[200] they must be scaled-up and reach all children. The Curriculum Development Department (under the Ministry of Education) would be well placed to develop a comprehensive and integrated syllabus, in collaboration with the Ministry of Health, child protection experts and early childhood professionals, and in consultation with other relevant stakeholders (e.g., religious groups, civil society organisations, etc.). The syllabus should be implemented in both public and private schools and in other educational institutions. The existing curriculum should be adequately funded and scaled-up at all levels, building on international guidance such as the UNESCO International technical guidance on sexuality education.[201]
- As school teachers are a preferred source of sex education, they should receive additional training on OCSEA and support to overcome challenges in teaching comprehensive sexuality education in schools. Teacher Training Institutions could introduce a comprehensive sexuality education curriculum into their syllabus along with fundamental training on gender-sensitivity and child psychological health. In addition, regular training on sexuality education could be included under the Ministry of Education's Continuous Professional Development programme to support continuous learning among teachers. This would ensure teachers are adequately qualified to deliver comprehensive sexuality education to children in schools.

The government body suggested to lead in implementing this recommendation is the Ministry of Education with the support of the Ministry of Health and the Ministry of Women, Family and Community Development. Non-governmental organisations could support delivery of these programmes to out-of-school children, marginalised children and children with disabilities.

200. Sex education through the Social and Reproductive Health Education curriculum ('Pendidikan Kesihatan Reproduktif dan Sosial' or PEERS) has been introduced into the primary and secondary school systems by the Ministry of Education, but its implementation is limited for various reasons, including a lack of sufficiently trained teachers and a lack of support from parents and the wider community. Furthermore, PEERS places strong emphasis on abstinence as the best policy. This approach or punitive measures do not confront the reality of adolescent sexuality. Other examples include the Federation of Reproductive Health Associations Malaysia which provides ad hoc workshops in schools on comprehensive sexuality education. The National Population and Family Development Board (LPPKN) under the Women's Ministry delivers comprehensive sexuality education informally via *Kafe at Teen* and their website.
201. UNESCO (2018). International technical guidance on sexuality education (revised edition).

2.2 Age-appropriate OCSEA education and awareness-raising approaches need to reach all children in Malaysia. The *Disrupting Harm* data did not indicate any differences according to age or gender in terms of the likelihood of children experiencing OCSEA, so programmes should target children of all genders and ages. Special care should also be taken to ensure that information is communicated to children whose situation may increase their vulnerability to OCSEA, including children with disabilities, children affected by migration, street-connected children, out-of-school children and children who experience other forms of violence.[202] Non-governmental organisations may be ideally positioned to deliver information to these vulnerable populations. This is not intended to place the burden on children to protect themselves, but rather to help them become aware of the risks.

There are other existing reports[203] and initiatives[204] developed internationally that might act as helpful references and examples of good practice in age-appropriate resource material.[205]

2.3 Support those with a duty of care for children – particularly caregivers, teachers, medical professionals and social workers – to overcome discomfort around discussing sex and sexuality in age-appropriate terms. This can encourage open dialogue about sexual abuse and exploitation online or in person. The data indicates that a proportion of children – particularly younger children aged 12–13 – would prefer to receive sex education from their caregivers. Guidance and skills-building for caregivers could be provided through existing government interventions and programmes promoting positive parenting.[206,207] Several guidelines exist, including a guide developed to assist UNICEF and its partners in supporting and implementing parenting interventions that prevent and respond to violence against children.[208]

Caregivers, teachers and social support services[209]

2.4 Learn about what children are doing both online and offline and be vigilant about the people that their children or the children in their community interact with. Consider whether these interactions seem appropriate for children. Because OCSEA affects children regardless of age and gender, caregivers and duty-bearers should be vigilant about *all* children's interactions regardless of their gender or gender identity.

2.5 Inform children about their right to be protected from all forms of emotional, physical and sexual abuse and exploitation, including OCSEA. Engage with children to build their understanding of how to stay safe by setting boundaries and recognising appropriate and inappropriate behaviour. Education and awareness-raising efforts should not focus disproportionately on 'stranger danger'. The data suggests that, in a proportion of cases, offenders are people known to the child – sometimes family members. Children should be made aware that all forms of sexual exploitation and abuse (both online and in person) are unacceptable, even if committed or facilitated by family members or trusted adults.

202. This aligns with the ASEAN RPA Activity 1.3.3: to ensure that the specific needs of vulnerable groups are appropriately integrated into the development and implementation of national policies and programmes aimed at tackling OCSEA; and Activity 6.2.2: to ensure targeted awareness-raising and digital-literacy interventions for all vulnerable children and high-risk groups.
203. United Nations Population Fund (UNFPA). (2021). My Body is My Own.
204. United Nations Girls' Education Initiative. (2020). Bodily autonomy and SRHR.
205. National Society for the Prevention of Cruelty to Children. (2017). Talk PANTS with Pantosaurus and his PANTS song #TalkPANTS – YouTube.
206. Nur Azira Fideyah Binti Abdullah et al. (2020). The role of parents in providing sexuality education to their children. Makara J Health Res. 2020;24(3):157–163doi: 10.7454/msk.v24i3.1235.
207. The Naungan Kasih positive parenting programme's sexual and reproductive health module covers the following topics: Discussion on sexual and reproductive child rights, sexuality and parents' role in sexuality education, activities on talking about puberty, safe/unsafe touch, intimate relationships, sexual consent, child marriage and disclosure of sexual abuse. Parenting programmes under LPPKN could include guidance for caregivers to discuss sexuality with their children in age-appropriate and accurate terms. Schools could also be mobilised through PIBG (parent–teacher association) to engage with parents through the Ministry of Education.
The National Unity and Integration Department runs programmes for and with the urban poor community and could act as a forum to educate parents and the community on the dangers of OCSEA and how to engage in open conversations with their children. All universities and colleges providing social work training should include sexuality education in the curriculum, enable social workers to understand the need to sensitise children and adults about knowing their body parts and functions and provide skills to intervene appropriately and professionally with victims.
208. UNICEF. (2020). Designing Parenting Programmes for Violence Prevention: A Guidance Note.
209. Government, intergovernmental agencies and civil society need to translate and convey these messages to reach caregivers, teachers and social support staff.

2.6 Facilitate access to trusted online sources of information for children as a complement to adult-led comprehensive sexuality education.[210] The data indicates that children – particularly older children and children living in rural areas – may be reluctant to seek sex-related information and advice from adults and may rely on their peers (32% of the children surveyed consulted their friends on sex-related matters) or may resort to seeking answers online. Social workers, teachers and other trusted adults should promote reliable online sources of information – such as the ACE website[211] or the ANA Chatbot[212] – among children. Content from promoted sources of information should be regularly monitored and updated.[213]

INSIGHT 3

Children mainly experienced OCSEA through the major social media providers, most commonly via WhatsApp, Facebook/Facebook Messenger, WeChat or Telegram.

Government

3.1 Consult with Internet service providers, law enforcement authorities, privacy experts and technology companies to develop realistic, mandatory regulations for filtering, removing and blocking CSAM, addressing grooming and live-streaming of sexual abuse and complying with legally approved requests for user information in OCSEA cases. Monitor for timely compliance and implement sanctions for failure to comply. Stakeholders may refer to existing regulations from other countries as examples of good practice when considering amendments to the legislation.[214]

3.2 Make it mandatory for online platforms to have clear and accessible mechanisms for children to report concerns. Platforms should detail in child-friendly terms what the process looks like *after* children make a report. Popular social media and instant messaging platforms should consider closer collaboration with existing specialised reporting mechanisms in the country.[215]

3.3 Promote awareness of OCSEA among relevant private sector entities including Internet and mobile service providers to enhance understanding of the risks to children and what they can do to combat OCSEA. Promote multi-sectoral initiatives in order to develop or strengthen internal child protection policies on internet and communications technologies actors, ensuring these are aligned with international standards. Existing guidelines can serve as a useful starting point.[216,217]

3.4 Engage with owners and proprietors of internet cafes and other computer rental shops to ensure adequate safeguards are in place. The *Disrupting Harm* data indicates that 39% of internet-using children go online from internet cafes. Support owners of these establishments in taking steps to protect children from harmful content or interactions online by installing pop-up blockers, limiting access to sites that are not age-appropriate for children and making referrals to authorities about suspected cases of child sexual abuse or exploitation, as per mandatory reporting under The Sexual Offences Against Children Act and the Child Act 2001.

210. United Nations Children's Fund. The Opportunity for Digital Sexuality Education in East Asia and the Pacific. UNICEF East Asia and Pacific, Bangkok, 2019.
211. The National Population and Family Development Board (LPPKN) also provides a SRHR curriculum through ACE Reproductive and Social Education, which is available online in both English and Malay, and is also delivered through their Kafe@Teens initiative available nationwide. LPPKN is an agency under the Ministry of Women, Family and Community Development.
212. The Federation of Reproductive Health Associations Malaysia and UNICEF Malaysia developed the ANA chatbot in 2021. It allows young people to obtain sexual reproductive health and rights information anonymously via web chat or WhatsApp. WhatsApp: +60 3-5633 7514
213. Government (including the Ministry of Education, the Ministry of Health, the Ministry of Women, Family and Community Development and the Ministry of Youth) in collaboration with civil society organisations and experts could constitute a body overseeing trusted and promoted online sources of information.
214. United Kingdom Online Safety Bill (Chapter 2).
The Australia Online Safety Act requires industry to develop new codes to regulate illegal and restricted content. This refers to the most seriously harmful material, such as videos showing sexual abuse of children.
The EU Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse establishing an obligation for providers to detect, report, block and remove child sexual abuse material from their services.
215. For instance, in Malaysia, Monsters Among Us has successfully integrated their Lapor Predator Chatbot with WhatsApp, increasing access for children and the public.
216. ITU and UNICEF (2015). Guidelines for Industry on Child Online Protection.
217. Online resources for the ICT sector can be found here.

Consider making licensing conditional on these safeguards. Internet cafes could also serve as avenues to disseminate information among children about online safety strategies, help-seeking and reporting mechanisms, and about practices that promote positive engagement with digital technologies.

The bodies suggested to lead in implementing these recommended actions are the Malaysian Communications and Multimedia Commission (MCMC), with the support of local authorities (e.g., local councillors).

Law enforcement

3.5 Liaise more closely with global technology platforms and build on existing collaborative mechanisms to ensure that the digital evidence needed in OCSEA cases can be gathered rapidly and efficiently, including in response to data requests, and that CSAM is promptly removed. Consider engaging global platforms through coalitions such as WePROTECT, to which many are already members.

Industry

3.6 Technology companies and online financial providers should consider **proactively detecting and eliminating CSAM**, and identifying grooming attempts and live-streamed child sexual abuse using technology such as PhotoDNA[218] and API Arachnid.[219] Guidance to help companies establish policies and practices to support the prompt and effective removal of child sexual abuse material exists.[220] Private sector entities should also consider engaging with existing networks for support, such as the Asia-Pacific Financial Coalition Against Child Sexual Exploitation.[221]

3.7 Make formal reporting mechanisms within social media and instant messaging platforms clear and accessible to children and detail in child-friendly terms what happens after children submit a report. Platforms and Internet service providers must respond rapidly to reports made by children and demonstrate transparency and accountability.

3.8 Improve cooperation between Internet service providers and law enforcement agencies by:

- Creating pathways for processing requests and collaborations.
- Training staff to respond to data requests for ongoing cases and minimising processing times.
- Providing the law enforcement authorities with any associated information they have that might help to identify offenders and victims in a timely manner.
- Detecting and removing OCSEA-related content on their servers.

3.9 Prioritise responding to data requests from the courts in cases involving children to help reduce the duration of trials. This could be done by having Internet service providers appoint a law enforcement liaison officer to be responsible for handling any data requests from law enforcement agencies to speed up the investigation and prosecution of OCSEA cases.

3.10 Prioritise children's needs in product development processes. Such designs must be informed by evidence on children's digital practices and their experiences of OCSEA, including the *Disrupting Harm* study.[222]

218. Microsoft PhotoDNA helps detect child abuse and assists in the detection, disruption of circulation and reporting for further investigation by law enforcement.
219. Canadian Center for Child Protection. (n.d.). Project Arachnid.
220. UNICEF and GSMA (2016). Notice and Takedown: Company policies and practices to remove online child sexual abuse material.
221. The Asia-Pacific Financial Coalition Against Child Sexual Exploitation is a platform for law enforcement, regulatory bodies, companies and non-profit organisations to share, leverage and collaborate against online child exploitation. APFC members include banks, credit card companies, electronic payments networks, online third-party payment systems, internet companies, technology companies, social networking platforms, industry associations, law enforcement agencies and NGOs.
222. A good starting point for exploration is the free tools made available by the Australian eSafety Commissioner and this framework developed by UNICEF.

INSIGHT 4

Children who were subjected to OCSEA tended to confide in people within their interpersonal networks, particularly a friend, siblings or caregivers. Helplines and the police were almost never avenues through which they sought help.

Government

4.1 Ensure reporting mechanisms are available and accessible to all children, including those who do not live at home or those who do not have trusted adults to confide in. The *Disrupting Harm* data indicates that a majority of formal reports to law enforcement were made by adults, or by children themselves with the support of an adult. A further consideration would be to streamline existing hotlines and helplines and to create one dedicated reporting portal/number for children, that is free, accessible nationwide 24/7, confidential and has trained personnel who can offer online counselling. The current government helpline, the Talian Kasih helpline, is not dedicated to children but is open to other vulnerable individuals, including adults. Evidence from *Disrupting Harm* suggests that there are a number of reporting mechanisms in Malaysia, yet not all are well-resourced or adequately visible. This may create confusion for children who are trying to seek help.

4.2 Raise awareness that existing helplines[223] can be a source of information about how to support young people subjected to OCSEA. Children may be more likely to confide in trusted adults or friends than to call a helpline. However, the data from *Disrupting Harm* shows that few caregivers (19%) would call a helpline should their child be subjected to sexual harassment, abuse or exploitation. Similarly, 56% of the children surveyed would not know where to go if they or a friend were sexually assaulted or harassed.

Awareness-raising efforts should communicate that peers, siblings, caregivers and teachers can find information, support services and help through helplines.

An important prerequisite is that helplines are adequately resourced and trained concerning OCSEA, so that they can provide good quality information and advice in a child-friendly manner. Employees and volunteers should be screened to ensure that they are fit to work with children and the government should consider the provision of psycho-social support to helpline staff who have constant exposure to trauma-inducing cases.

Awareness-raising programmes may include advertising helplines and the support services they offer at bus stops and on social media, and incorporating messages into child protection awareness messages from relevant government ministries and their partners. Messages can also be disseminated through schools and places of worship, and community volunteers can be trained to disseminate these messages at the community level. Messages should be targeted to all communities including the most marginalised.

The government agencies that should be involved in the implementation of this recommendation include the Ministry of Women, Family and Community Development, the Ministry of Education, the Department of Social Welfare Malaysia, and the Malaysian Communications and Multimedia Commission and CyberSecurity Malaysia under the Ministry of Communication and Multimedia.

4.3 Given that children rely heavily on their interpersonal networks for support, especially friends, consider expanding programmes such as the S.C.A.R.S programme[224], the Federation of Reproductive Health Associations Malaysia's Reproductive Health of Adolescents Module and Life's Journey programmes,[225] which rely on opening dialogue among young people and encouraging peers to seek help for abuse. Such initiatives could improve children's awareness of OCSEA and increase rates of disclosure.

223. Existing helplines in Malaysia include The Talian Nur Helpline, the Childline Talian Kasih 15999 hotline, National Helpline Childline Malaysia, The Protect and Save the Children (P.S. The Children) Hotline and the Lapor Predator Reporting Portal.
224. Childline Foundation. (n,d). Programmes.
225. The Federation of Reproductive Health Associations, Malaysia (FRHAM) strongly advocates for rights-based, gender-focus and informed-choice CSE. Modules such as the Reproductive Health of Adolescents Module (RHAM) and Life's Journey were developed for this purpose. The federation believes in meaningful youth participation and adopts youth-friendly services and youth-led projects in their programmes.

4.4 Dedicate resources to child helplines and CSAM hotlines to improve record keeping so that they can record statistics on the OCSEA cases reported to them. Increasing the capacity of these organisations to collect and analyse such data will provide a better understanding of children's experiences of OCSEA, including how it changes over time, which could help develop prevention programmes and the necessary policies and legislative amendments.

4.5 Invest in improving the capacity of all staff working in social support services (including professionals working in health institutions, education institutions, social welfare institutions, rehabilitation and recovery centres and those providing psycho-social support) to recognise the unique risks and harms associated with OCSEA, and to better identify children at risk or that have experienced OCSEA. Training of staff working at the district level should be prioritised as they are the first level of contact and support for victims of OCSEA and their families. Training should also be provided to the secretariat of the Malaysian Council for Anti-Trafficking in Persons and Anti-Smuggling of Migrants to better identify OCSEA cases. The Child Act[226] imposes mandatory duties on these professionals to report incidents of child sexual abuse, including OCSEA. In addition, the Sexual Offences against Children Act[227] imposes a more general mandatory reporting duty that requires any person (whether a professional or a private citizen) to report any offence outlined in the act (which includes OCSEA).

It is, therefore, important that these professionals are equipped with the necessary knowledge to recognise OCSEA and other forms of abuse when they occur. Government agencies that should be involved in the implementation of this recommendation include the Ministry of Women, Family and Community Development and the Ministry of Health through the Suspected Child Abuse and Neglect (SCAN) teams under government hospitals, which can build the capacity of the multi-disciplinary teams on OCSEA.

Caregivers, teachers and social support services[228]

4.6 Responses to disclosures of OCSEA should always convey that the abuse is never the child's fault, whatever choices they have made; it is always the fault of the offender or exploiter of the child.

Data from the household survey showed that 78% of children and 83% of caregivers believed that it is the victim's fault when a self-generated image or video is shared further. Reasons commonly cited by children for not disclosing instances of OCSEA included feeling that they had done something wrong or fear of getting into trouble or creating trouble for the family.

All responses to and interactions with children impacted by OCSEA should be without judgement or punishment.[229]

4.7 Avoid restricting children's internet access as a response to potential harm and, instead, take an active role in children's internet use and provide them with support and information on how to stay safe online. Over a third of the caregivers surveyed in Malaysia said that they would restrict their child's internet access if he/she was upset by something online. This can have a negative impact on children's digital skills and might be perceived by children as a punishment and so reduce the likelihood of them disclosing such matters in the future.

4.8 Help children, caregivers, teachers and those working with children to understand the full extent of the risks of sharing sexual content online, including the possibility of the content being shared further and of sexual extortion, and how to engage in harm minimisation to limit possible negative repercussions. Only 1% of children in the household survey said that they had shared sexual images of themselves online, but 17% did not regard this as 'very risky'.

226. Government of Malaysia. (2001). Laws of Malaysia - Act 611 - Child Act 2001, as amended in 2017, Sections 27, 28 and 29.
227. Government of Malaysia. (2017). Laws of Malaysia – Act 792 - Sexual Offences against Children Act 2017, Section 20.
228. Government, intergovernmental agencies and civil society need to translate and convey these messages to reach caregivers, teachers and social support staff.
229. See for example WHO Guidelines for the health sector response to child maltreatment.

INSIGHT 5

A range of promising initiatives driven by the government, civil society and industry are underway in Malaysia, but weak inter-agency coordination and cooperation and limitations in budgetary resources exist.

Government

5.1 Consider expanding/including the role of the multi-stakeholder committee (Integrated Action Committee on the Management of Children's Issues Online) led by the Ministry of Women, Family and Community Development in general child online protection work, including reviewing and implementing the Disrupting Harm findings.

5.2 Address the challenges faced by OCSEA victims and their caregivers within the criminal justice system that lead to them either withdrawing registered complaints or settling OCSEA cases with the offender informally out of court. Victims of sexual crimes may choose not to pursue prosecution for various reasons, such as the length of period it takes to finalise a criminal case against the offender or the shame and stigma that is often associated with sexual crimes. Addressing these underlying challenges will ensure that more OCSEA cases that are reported to the police result in the prosecution of offenders. The government representatives interviewed for *Disrupting Harm* indicated that, since the enactment of the Sexual Offences against Children Act in 2017, few cases of OCSEA reported to the police have culminated in the prosecution of the offenders due to the withdrawal of registered complaints by child victims and the settling of cases outside the formal justice system.

5.3 Allocate financial resources to support ordinary courts, including the court for children, in order to achieve the same level of child friendliness as the special courts, which were established to handle sexual crimes against children. Data from *Disrupting Harm* revealed that the specialised courts provide better services to child victims of sexual crimes than ordinary courts as they have child-friendly facilities, such as private entrances and exits for child victims, child-friendly waiting rooms and video link facilities. Ordinary courts do not always have these child-friendly facilities. Currently, however, there are only two special courts, in Putrajaya and Kuching, and the initiative has yet to be expanded to other states.

5.4 Equip more judges, prosecutors, law enforcement officers and social workers, including those working in ordinary courts, with the technical knowledge and skills necessary to handle OCSEA cases and to work with child victims and witnesses in a child-friendly manner within the criminal justice system, and ensure that child-friendly procedures are implemented whenever and wherever children are involved as victims in the justice system. This can be done by:

1. Institutionalising capacity-building initiatives as part of the training calendar of the government. This will ensure that the necessary resources are secured and a regular and recurring budget is allocated.
2. Develop standard modules on OCSEA and child-friendly measures that can be used by trainers. These can also be integrated in the training curricula of the judicial and legal training institute and the Police Training Academy.
3. Child-friendly facilities (such as the ones implemented in the special courts for Sexual Offences against Children) should be made available to all courts that work with children The court methods used in the Barnahus[230] model may also be explored for adoption.

230. See: Child-friendly centres for abuse victims: Barnahus.

Government agencies that should be involved in the implementation of this recommendation include the judiciary, the Attorney Generals Chambers, the Ministry of Women, Family and Community Development, the Judicial and Legal Training Institute, the Department of Social Welfare Malaysia, the Royal Malaysia Police and the Ministry of Health.

5.5 Support all child victims of OCSEA in accessing support services including 'legal companion' services and medical services. Improve uptake of legal companion services by increasing awareness of this service among justice professionals and members of the public. For medical services, referral pathways from district/community clinics to One-Stop Crisis Centres should by strengthened by updating and training all medical staff at district and community clinics using the "Ministry of Health – One Stop Crisis Centre: Policy and Guidelines for Hospitals".[231] These guidelines serve as interagency standard operating procedures to guide health workers when providing medical services to child victims.

5.6 Adopt and implement the Malaysia Cyber Security Strategy for 2020–2024, which includes initiatives to increase the knowledge and skills of law enforcement officers and other criminal justice professionals, including members of the judiciary, with respect to cybercrime.

Caregivers, teachers and social support services[232]

5.7 Provide all staff working in social support services (including professionals working in health institutions, education institutions, social welfare institutions, and rehabilitation and recovery centres) with evidence-based best practices for responding. This could be done by incorporating information on OCSEA into the existing child protection social services training. When children are brave enough to seek help, those they seek help from must be equipped to support them.

Law enforcement

5.8 Increase the priority attached to OCSEA by the political authorities and law enforcement machinery when investing in talent and resources. Efforts to highlight the threat of OCSEA in Malaysia may enable the D11 division/Malaysia Internet Crimes Against Children (MICAC) Investigation Unit to attract the additional resources required to more effectively combat these crimes.

5.9 Strengthen the Malaysia Internet Crime Against Children (MICAC) Investigation Unit with sufficient personnel and the necessary expertise to address OCSEA, and reconnect to INTERPOL's International Child Sexual Exploitation database. The small number of staff in the specialised unit adversely affects the prompt investigation of cases and evidence building. The unit is not optimally staffed to handle the sheer volume of CyberTips from NCMEC. The team also needs reinforcement in terms of cybersecurity experts and infrastructure. Government representatives and justice professionals who were interviewed were of the view that law enforcement staff's OCSEA training is currently insufficient.

5.10 Ensure vertical, horizontal and cross-sectional collaboration as a prerequisite to effective operations using standard operating procedures. Limited information was available on the local sub-national units. Although the Malaysia Internet Crimes Against Children Investigation Unit has personnel who provide field support, INTERPOL was not able to interview them.

5.11 Further enhance international cooperation among law enforcement agencies. While Malaysia's cooperation and coordination with international law enforcement bodies is commendable and it has collaborated successfully with foreign law enforcement agencies, there is scope to extend the level of international cooperation.

5.12 Psychological support for the staff members of the Malaysia Internet Crimes Against Children Investigation Unit and other pertinent units would also help to improve the effectiveness with which they conduct stressful investigations and serve the community.

231. The Ministry of Health Malaysia. (2015). One Stop Crisis Centre: Policy and Guidelines for Hospitals.
232. Government, intergovernmental agencies and civil society need to translate and convey these messages to reach caregivers, teachers and social support staff.

5.13 Ensure that the Malaysia Internet Crimes Against Children Investigation Unit plays a meaningful role in the drafting, finalisation and implementation of preventive policies, including the upcoming National Child Protection Policy and Action Plan, in order to benefit from the interest, engagement and investment of its staff in the digital safety of children.

5.14 Standardise the utilisation of the Child Interview Centres by law enforcement officers when interviewing child victims of OCSEA and other forms of sexual abuse. Although the criminal justice professionals interviewed for *Disrupting Harm* explained that there are Child Interview Centres in every state in Malaysia, they also indicated that these centres are not always used.

Justice professionals

5.15 Ensure that criminal justice professionals have a standard information package to provide to all victims and their caregivers related to child sexual exploitation and abuse (including OCSEA). The package should clearly inform children about their rights, including their right to compensation, and familiarise them with the procedures they will encounter. This will enable child victims and their caregivers to make informed decisions.

5.16 Prevent the re-traumatisation that occurs when victims are repeatedly summoned to provide information during investigations and as a result of exposure to the offender during trials. The pre-recording of the full child witnesses' testimony prior to trial, in a child-sensitive environment, should be considered so that the child does not need to attend the trial.

5.17 Deputy prosecutors must support victims to obtain compensation by ensuring that they submit the necessary applications for it in court. According to the criminal justice professionals interviewed for *Disrupting Harm,* deputy public prosecutors are responsible for submitting applications for compensation to the court on behalf of victims, but they do not always do so. Without the submission of these applications, the court cannot order the offender to compensate a victim of OCSEA.

INSIGHT 6

Although existing legislation, policies and standards in Malaysia include provisions relevant to OCSEA, including strong provisions regarding child-friendly investigations and prosecutions, support to implement such standards across the country and further legislative reform are needed to ensure a comprehensive response to OCSEA.

Government

6.1 Although provisions on child sexual abuse material can be used in cases of live-streaming of child sexual abuse, the legislation should be amended to **criminalise live-streaming of child sexual abuse as a separate and distinct offence.**

6.2 Expand the existing provision criminalising those who threaten to use CSAM to specifically refer to the act of using such material to extract sexual content or other benefits from a child, i.e., the sexual extortion of children committed/facilitated in the online environment.

6.3 Strengthen the implementation of the Sexual Offences against Children Act by monitoring its implementation in order to identify and address any obstacles that hinder its effectiveness. Findings from *Disrupting Harm* indicate that cases of OCSEA are sometimes prosecuted under provisions criminalising homosexuality (Sections 377A and 377B of the Penal Code) instead of under the relevant provisions of the Sexual Offences against Children Act. The Government agency that should lead the implementation of this recommendation is the Attorney General Chambers.

6.4 Amend legislation to ensure that provisions establishing age of sexual consent are consistent across legislation and apply equally to boys and girls. A close-in-age exemption should be provided for consensual sexual relationships between adolescents.

6.5 Amend legislation to ensure children are exempt from criminal liability for the self-generation of sexual content.

6.6 Include a provision in the legislation prohibiting sex offenders from **holding positions involving or facilitating contact with children and introduce an obligatory check against the sex offender registry.**

6.7 Consider legal amendments to align with international conventions that offer excellent guidance for addressing this issue – such as the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention) and the Convention on Cybercrime (the Budapest Convention) adopted by the Council of Europe. Although these conventions are regional commitments for member states of the Council of Europe, the guidance they provide on OCSEA is highly relevant. While it may not be required for states outside this region to comply with these conventions, they are a useful measure of national legal frameworks related to OCSEA and they are open for accession by states that are not members of the Council of Europe.

6.8 Ensure the creation of a roadmap towards the implementation of the updated National Child Policy and Action Plan under the Ministry of Women, Family and Community Development. Following the ongoing review of the Plan of Action on Child Online Protection (2015–2020) and other child protection and child development policies, such as the 2009 National Child Protection Policy and the 2009 National Child Policy, an action plan/roadmap on child online protection should include a coordination mechanism with relevant stakeholders and a monitoring and evaluation plan. The said proposed action plan could build on existing regional and global guidelines, such as the WePROTECT Model National Response and the ASEAN Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN.

6.9 Support the implementation of existing policies on child protection and child development by allocating the required financial and human resources necessary for their implementation and building the capacity of relevant government agencies for their respective roles in implementing these policies. The government representatives interviewed indicated that the main challenges facing government agencies in the implementation of policies were limited financial resources and a lack of trained personnel to effectively implement policies and plans. It was highlighted that, in general, the various policies related to child protection and child development are not adequately incorporated in government decisions. The government agencies that should be involved in the implementation of this recommendation include the Ministry of Women, Family and Community Development, the Ministry of Finance, the Ministry of Education, the Ministry of Health and the Attorney Generals Chambers.

6.10 Join the WePROTECT Global Alliance and use the Model National Response to Preventing and Tackling Child Sexual Exploitation and Abuse to help organise the national response to OCSEA. The Model is a valuable tool for governments to improve the level of their response.

The government agencies that should be involved in the implementation of this recommendation include the Malaysian Communications and Multimedia Commission, the Ministry of Women, Family and Community Development and Cybersecurity Malaysia.

ACKNOWLEDGEMENTS

INTERPOL, ECPAT International and UNICEF Office of Research – Innocenti have appreciated the unique opportunity to work shoulder-to-shoulder to assess OCSEA in Malaysia. This comprehensive report is the result of a two-year collaborative effort to design research, gather data and produce extraordinary evidence. These efforts would not have been successful without the engagement of so many people and partners in Malaysia. First and foremost, our biggest thanks go to the children who contributed – especially the young people who experienced OCSEA and courageously spoke about it with the research teams. The experiences of children are key to understanding and guiding our way forward. The project partners would also like to express their appreciation to the *Disrupting Harm* Technical Working Group, chaired by the Malaysian Communications and Multimedia Commission, and to everyone who engaged with *Disrupting Harm* by:

Contextualising the findings:

Association of Registered Childcare Providers Malaysia; Attorney General's Chambers (AGC) Malaysia; Bar Council Malaysia; Be My Protector; Childline Foundation; CRIB Foundation; the Department of Syariah Judiciary Malaysia; The End CSEC Network Malaysia; the Malaysian Federation for the Deaf; Federation of Reproductive Health Associations, Malaysia; The Fourth; Global Shepherds Berhad; Hospital Selayang; Hospital Tunku Azizah; Human Rights Commission Malaysia (SUHAKAM); the International Justice Mission (IJM) Center to End Online Sexual Exploitation of Children; Maestral International; the Malaysian AIDS Council; the Malaysian Association of Social Workers; the Malaysian Child Welfare Council; the Malaysian Communications and Multimedia Commission; Malaysian Crime Watch – MyWatch; the Ministry of Communication and Multimedia (K-KOMM); the Ministry of Education; the Ministry of Health; the Ministry of Housing and Local Government; the Ministry of Rural Development (KPLB); the Ministry of Women, Family and Community Development; the Ministry of Women, Early Childhood and Community Wellbeing Development, Sarawak; Monsters Among Us: Youth Advocates; the National Council of Welfare and Social Development Malaysia; the National Cyber Security Agency; the National Population and Family Development Board (LPPKN); the Office of the Children's Commissioner (OCC), the Human Rights Commission of Malaysia (SUHAKAM); the Organisation of Islamic Cooperation Independent Permanent Human Rights Commission; Persatuan Cakna Anak Malaysia; Petaling Jaya Child Council; Protect and Save the Children; Reproductive Health Association Kelantan (ReHAK); Royal Malaysia Police (PDRM); UNHCR Malaysia; UNICEF Malaysia; UNICEF East Asia and Pacific Regional Office; Universiti Malaya Women's Aid Organisation; Vanguards for Change; Women's Centre for Change (WCC) – Penang.

Supporting data collection: The Department of Statistics Malaysia; Ipsos Malaysia; Ipsos MORI; the Malaysian Communications and Multimedia Commission; Ministry of Health Malaysia; UNICEF East Asia and Pacific Regional Office; UNICEF Malaysia; Dr. Raj Abdul Karim (End CSEC Network Malaysia).

Sharing expertise and experiences through interviews and surveys: the Ministry of Women, Family and Community Development; the Legal Affairs Division, Prime Minister's Department; the Legal Affairs Division, CyberSecurity Malaysia; the Ministry of Education; the Ministry of Health; the Department of Social Welfare; Attorney General's Chambers Malaysia; the Malaysian Communications and Multimedia Commission; the Sexual, Women and Child Investigations Division (D11), Royal Malaysia Police; the Human Rights Commission of Malaysia (SUHAKAM); the National Population and Family Development Board; the Ministry of Home Affairs; General Welfare Department for Sabah (State Government); Sexual Crime Court Against Children; the Legal Aid Department; Prime Minister's Office; Voices of the Children; Protect And Save The Children; the Social Welfare Department. Selangor; the Welfare Department, Kuala Lumpur; Women's Centre for Change (WCC); the Court of Children in Kuala Lumpur; Global Shepherds Berhad; Women's Aid Organisation; Child and Adolescent Psychiatry Unit, Hospital Tuanku Azizah (previously known as Women and Children Hospital, Kuala Lumpur); the Suspected Child Abuse and Neglect (SCAN) team, Hospital Kuala Lumpur (HKL); Yayasan Chow Kit (YCK); Rohingya Women Development Network; Malaysian Social Research Institute (MSRI).

Reviewing key recommendations:
Dr. Raj Abdul Karim (End CSEC Network Malaysia), Amy Bala (Malaysian Association of Social Workers), Amanda Bissex (UNICEF Malaysia), Saskia Blume (UNICEF Malaysia), Shelley Casey (UNICEF Malaysia), Dr Farah Nini Dusuki (Universiti Malaya), Lyn-Ni Lee (UNICEF Malaysia), Adam Ling (UNICEF Malaysia), Tiffany Mervin (UNICEF Malaysia), Thulasi Munisami (Protect and Save the Children), Indra Kumari Nadchatram (UNICEF Malaysia), Dr. Rajeswari Nagaraja (Federation of Reproductive Health Associations Malaysia), Firzana Redzuan (Monsters Among Us), Dato Yasmeen Mohd Shariff (Bar Council Malaysia, Child Rights Committee), Sivaselvi Supramaniam (UNICEF Malaysia), Marc Vergara (UNICEF Malaysia)

Without the collaborative effort of all the staff, consultants, translators and interns involved in the reports, this tremendous piece of research would not have come together. In particular, we would like to thank:

ECPAT International: Tiago Afonso, Dr Victoria Baines, Alice Beaven, Will Beaven, Rebecca Boudreaux, Willy Buloso, Yermi Brenner, Dr Mark P. Capaldi, Narciso Cumbe, Dr Dorothea Czarnecki, Jarrett Davis, Rangsima Deesawade, Julia Durska, Sonia Espallargas Val, Anneka Farrington, Liam Foley, Beatrice Gacengo, Thiyagu Ganesan, Dr. Susanna Greijer, Zipporah Goetze, Josefin Hagstrom, Alastair Hilton, Maria Ibañez Beltran, Worrawan Jirathanapiwat, Supriya Kasaju, Dr Mark Kavenagh, Bernard Kennedy, Dorine van der Keur, Susan Kreston, Guillaume Landry, Marie Laure Lemineur, Raphaelle Lecler, Katrina Mariswamy, John McGill, Mark McKillop, Stella Motsi, Florence Mueni, Thomas Müller, Manida Naebklang, Cathrine Napier, Rumbidzai Ngindi, Freddie Nickolds, Megan Northey, Esther Obdam, Dr Nativity Petallar, Dr Kirsten Pontalti, Marie Joy Pring, Dr Ethel Quayle, Marita Rademeyer, Kieran Rumsby, Jennifer Schatz, Guncha Sharma, Nong Socheat, Chitrapon Vanaspong, Andrea Varrella, Kirsten Walkom, Timothy Williams.

UNICEF Office of Research – Innocenti: David Anthony, Dr Daniel Kardefelt-Winther, Marie Nodzenski, Marium Saeed, Rogers Twesigye.

INTERPOL's Crimes against Children Unit.

The partners also acknowledge the guidance of the Panel of Advisors and the extraordinary financial investment in this project from the Global Partnership to End Violence against Children, through its Safe Online initiative. The *Disrupting Harm* partners are grateful to the Safe Online team for its conceptualisation of *Disrupting Harm*, its technical contributions and its unwavering support.