Updated 2026

Cybersafety:
Keeping Children Safe Online

Guidebook for Teachers and Parents

WCC
Women's Centre for Change

Cummins

Produced and Published by
Women's Centre for Change, Penang
241, Jalan Burma, 10350 Penang, Malaysia
04-228 0342 011-3108 4001
www.wccpenang.org
WCC Penang

First Edition, 2021
Updated Edition, 2026

Supported by
Cummins Inc.

Written by
Dato' Dr Amar-Singh HSS
Consultant Paediatrician

Compiled and Edited by
Ambiga Devy, Nadila Daud, Loh Cheng Kooi,
Yeap Yen Ying, S. Mangleswary & S. Hastiny

Updated in 2026 by
Yeap Yen Ying, Choong Yong Yi,
Loh Cheng Kooi & S. Hastiny

Illustrations by
Faizati Mohd Ali

Designed and Layout by
Elaine Thniah, C-Square Sdn Bhd

Printed by
Phoenix Printers Sdn Bhd

ISBN No: 978-967-16908-9-5

Soft copy is available here:

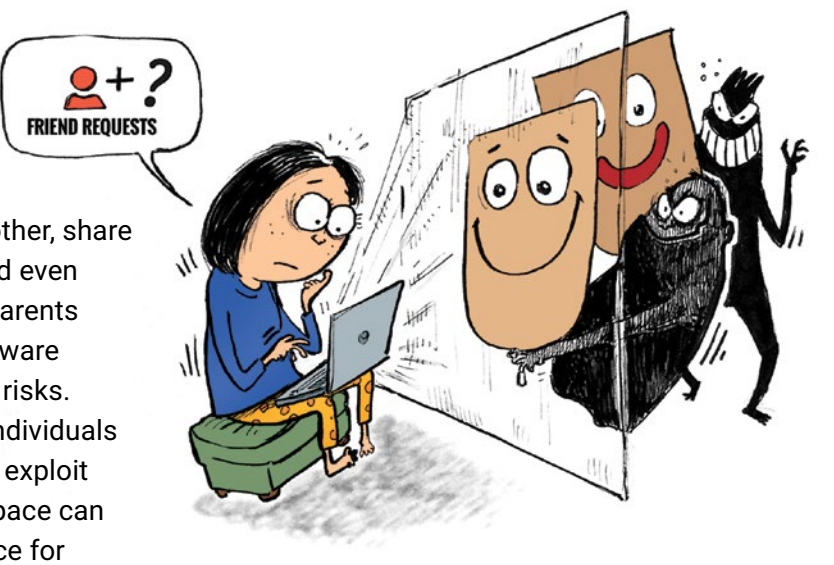
Click for "Cybersafety Guidebook"

CONTENTS

1.0 Introduction to Online Sexual Abuse of Children*

The Internet is a remarkable tool which provides and shares information, offers education and connects individuals and groups. Hundreds of millions of people use it every moment and this includes children. It is estimated that as of October 2025, there were 6.04 billion active internet users worldwide which amounts to 73% of the global population. Of this total, 5.66 billion (68%) of the world's population were social media users and more than 90% accessed the internet via mobile devices[1].

One of the greatest uses of the internet is for interaction. Cyberspace has become a place where children meet and make friends. It is where many children share their lives with their friends. Most do so using a mobile device, usually a hand phone, via a variety of social media applications like Snapchat, Instagram, Twitter, TikTok, Facebook, Reddit, or peer-to-peer messaging applications like WeChat, WhatsApp, Telegram, etc. New applications are being designed all the time and some will be adopted by children.



Many of the interactions on social media or peer-to-peer messaging are useful and help children keep in touch with each other, share ideas and information and even support each other. But parents and children need to be aware that the internet also has risks. Unfortunately, there are individuals online who are looking to exploit others and hence cyberspace can become a dangerous place for children and adults. We need children to be able to discern which are healthy and which are harmful interactions, so as to protect themselves.

*By law, children are defined as persons below the age of 18 years.

[1] Statista https://www.statista.com/statistics/617136/digital-population-worldwide/

One harmful interaction is the online sexual abuse of children. Online child abuse is sometimes called 'cyber violence' or 'online sexual exploitation'. It happens on digital platforms (i.e. not physical) or at a distance and can be anonymous. Harmful individuals attempt to make contact with children for sexual purposes and target social media sites that are popular among children, sometimes impersonating a child.

Online sexual abuse takes many forms including grooming, sexting, sextortion, cyber-stalking, harassment, bullying and doxxing. The perpetrator (person who commits the crime) could be a stranger or someone who knows the victim. At times, more than one perpetrator could be involved. These perpetrators, often men, are quick to take advantage of the Internet and online tools to victimise children. They can be very manipulative and persistent. With the development and widespread use of artificial intelligence (AI), a new threat for online child sexual exploitation and abuse has emerged - generative AI. Generative AI can be misused to create texts, images and videos that depict or facilitate child sexual abuse materials.

Similar to physical sexual abuse, online sexual abuse can hurt and damage children emotionally and physically for life. However, unlike physical abuse, in online abuse, the person can be re-victimised many times over if an image, video or story is shared widely on digital platforms.

Online sexual abuse can happen to both boys and girls. Studies on cyber-bullying of Malaysian children show that one in three have been victims of cyber-bullying[2]. Thirty percent of girls report that they have been sexually harassed in chat rooms[3]. Victims of online sexual abuse often are ashamed of their situation and try to hide it from others but this only worsens the abuse and prolongs it. In one study, only half of children aged 12-18 years who were cyber-bullied spoke to their parents and asked for help[4]. It is also of concern that one in five school-going teenagers reported they had been involved in cyberbullying activities (22.7% boys, 13.9% girls).[5]

---

[2] Microsoft Corp. Global Youth Online Behavior Survey. https://www.digitalnewsasia.com/testing123

[3] Azizan, 2012. https://www.thestar.com.my/News/Nation/2012/04/29/Do-you-know-who-your-kids-are-talking-to/

[4] Telenor Group, 2016. https://www.telenor.com/media/press-release/safe-internet-research-spotlights-student-experiences-with-cyber-bullying-and-online-peer-pressure?pdf=print

[5] National Health and Morbidity Survey 2022 https://iku.gov.my/images/nhms-2022/1a_Infografic_AHS_BI_15062023.pdf)

While governments recognise the problem and have attempted to pass legislation to combat it, the sheer volume of online interactions makes policing extremely difficult. Hence prevention must involve training teachers and parents and offering appropriate education to children. Just as we would not allow a pre-school child to cross a road alone or go on a date with an unknown person, it is important that we are aware of who our children are interacting with when they are online.

Impact of Online Sexual Exploitation on Children

Online sexual abuse is just as harmful as sexual abuse that occurs offline or physically. The emotional and psychological impact on the child is devastating. Often adults tend to underestimate the effect of online sexual abuse on children and think that, because of 'non-contact', it cannot be severe. Most children who were traumatised have increased risk of anxiety, depression, eating disorders, post-traumatic stress symptoms and problems with establishing good relationships. Some have suicidal thoughts and may actually act on it.

Online abuse may be confusing to children. They may feel guilty for not being able to stop the abuse as well as 'having done the abuse to themselves' (asked to take off their own clothes by perpetrators and perform sexual acts on themselves). Unlike physical abuse, one very damaging aspect of online sexual abuse is that often pictures or videos are taken or shared. If these are shared online widely, the child can be re-victimised many times over. They may feel violated again and again, each time another person shares or downloads and looks at these images. In a sense the memory of their shame is 'immortalised' online – a never-ending abuse. Any attempt at healing must deal, not just with the impact of the trauma on the abused, but also the pain that comes from ongoing distribution. Otherwise there will be lack of closure in the recovery process.[6]

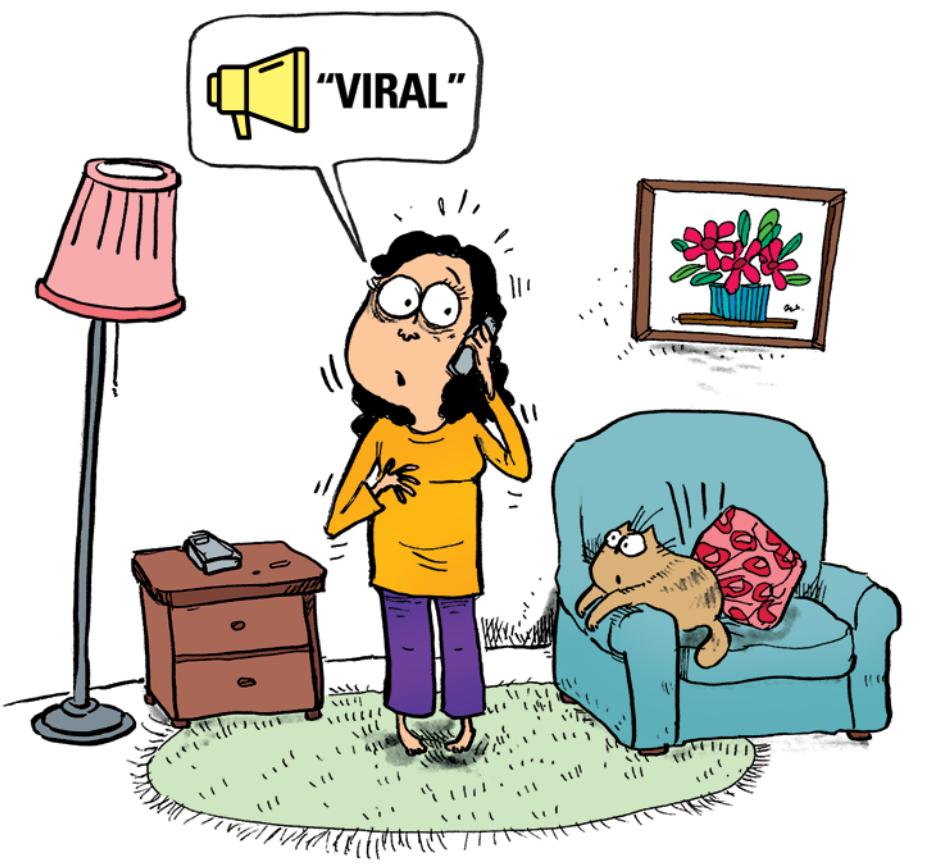
---

[6] Malin Joleby, Carolina Lunde, Linda Jonsson. *Understanding Online Child Sexual Abuse and How to Talk to Children about It.* The Inquisitive Mind. 2018 (38). https://www.in-mind.org/article/ understanding-online-child-sexual-abuse-and-how-to-talk-to-children -about-it

Understanding Why Children Get Trapped Online

Most children are naturally curious to explore our world and have a desire to establish friendships. In the 'traditional' face-to-face physical meeting, children and parents have more control on how the relationship can develop. They can physically see and communicate with the person, can rely on non-verbal cues and the identity of the person is generally not hidden. Parents can also play a larger controlling and protective role in who their child is making friends with. Much of these safety checks are not available when children are relating online.

It is difficult to distinguish different types of people online, i.e. are they safe, real friends or online strangers wanting to take advantage of the child. The identity of the person is uncertain. The 'privacy' that online communication allows also limits the support parents can give to their children as they negotiate the difficulty of establishing relationships. It is always best to train and encourage our children on how to recognise whether the online 'friend' is a trustworthy one. Even adults need such discernment, as we can see from the frequent online scams that occur.



It is at times difficult for adults to understand how and why children get caught up in such damaging contact. It is important to recognise that perpetrators are determined, persistent and subtle. They will often try many different strategies to ensnare children. They also share their successful modus operandi with other perpetrators. We need to realise that children are naturally curious about sexuality. Yet we do not teach them enough about it, and are not open enough to discuss sexual issues. Hence, they are exploited by perpetrators. Perpetrators use the child's curiosity and desire for connection with others to entrap them.

One often used method is to ask the child for a compromising image of herself/himself which is later used to intimidate or pressure the child by threatening to share it with others. The child then gets caught in a 'shame trap' – she/he feels responsible for the situation and is frightened to tell others because of the embarrassment and gets sucked deeper into the perpetrator's grasp. If children are brought up in homes or environments where they are able to talk about their feelings of guilt and shame, then asking for help is easier; otherwise they suffer in silence.

This guidebook on Cybersafety is aimed at helping children make good decisions when being online so that they can use the internet safely. It describes the common types of online sexual abuse and offers suggestions on how to deal with it. It is to be used as a training module with children in schools or even by parents at home.

This guidebook covers the following areas:

- Types of online sexual abuse
- What to look out for
- Handling disclosure
- Activities to educate children on online sexual abuse
- List of related laws and useful contacts

Remember, just because we do not discuss these issues does not mean they are not happening to our children. It is critical that we educate our children about online abuse. In so doing, we can reduce their vulnerability and prevent them from becoming exposed to online child sexual abuse.

2.0 Types of Online Sexual Abuse

This section describes the types of online sexual abuse, explains the terminology used, outlines how perpetrators work, the impact on children and what our laws say about it.

Online Grooming of Children for Sexual Purposes

Online grooming of children for sexual purposes is the development of a friendship with a child online with the purpose of sexually abusing them. Harmful adults may impersonate a child and navigate social media sites with the view of establishing a relationship with them.

Once a relationship has been established, the perpetrator will induce the child to spend time online alone with her/him and engage in a variety of sexual activities like sexting, sextortion, live streaming the child 's naked body, or even arranging to meet in person to sexually assault them. They may also share the child's sexually explicit images or videos with others. As social media usage has grown in the past decade, online grooming of children for sexual purposes has significantly increased. Online grooming can involve both girls and boys.

Examples

Grooming is a common technique used by online perpetrators. The common example is a child who is approached or meets a 'nice person' in a chat room. This individual is a very good listener, seems to understand her/his loneliness and is always appreciative. The child gradually develops a private friendship with this person who then exploits her/him.

How Online Groomers Work

1. Groomers target social media sites where children hang out. They often target children who are looking for attention or affection, who are less supervised by their parents or adult carers, and who can use the internet without supervision.
2. They may pretend to be someone else by using fake identity.
3. In the initial stages the perpetrator seems extremely nice and caring, and hence the child welcomes this attention. Once they have established initial contact on a social site or forum they move the conversation to a one to one location, e.g., direct messaging.
4. They build trust by being very charming, understanding and listening to the child a lot. They may also pretend to have shared interests or past experiences. They often meet a 'need' in the child for attention or someone who 'understands' her/him. Common grooming strategies include giving attention, flattery, offering confiding information, sending special gifts and promising an 'exclusive relationship'.
5. They will gradually attempt to obtain the child's personal details like name, address, hand phone number, etc.
6. The groomer may try to introduce more sexual related elements into the relationship and try to desensitise the child to sexual images and activities. They aim to gain some control over the child.
7. Gradually they become more manipulative and start to request sexually related images or videos.
8. Once the perpetrator has a 'hold' on the child, the tone of the relationship changes to one of intimidation, demands and abuse.
9. They may request a meeting via online video calls and ask the child to undress or perform sexual acts. An element of blackmail or sextortion may occur.
10. A key element of grooming is to ensure the child's secrecy in the online relationship. They maintain the child's silence and commitment to secrecy by using emotional blackmail.
11. Some will request a private, in-person meeting where physical sexual abuse may occur.
12. Note that the perpetrator may be working alone or be part of a group of individuals.

Impact

There is evidence to suggest that children who are groomed and subsequently sexually abused online suffer the same harm as those who are sexually abused physically. The child retains the shame of what has happened and the guilt of allowing it to occur. Many suffer long term depression and some may resort to self-harm. A key long-term impact is the damage done to the child's ability to form trusting relationships with others, especially if her/his family was unsupportive or unresponsive when the abuse was discovered.

Relevant Sections of the Law

Sexual Offences Against Children Act 2017

Child grooming (Section 12)

Section 12 prohibits child grooming such as the use of social media to befriend a child with the intention of using the child to create child sexual abuse materials or to commit a sexual offence. It is illegal for any person to communicate by any means with a child with the intention to commit any offence under the Act, even if they never actually meet, and upon conviction, can be punished with imprisonment for a term not exceeding 5 years and liable to whipping.

Meeting following child grooming (Section 13)

Section 13 provides for heavier penalty if there is any meeting following child grooming. Any person who, having communicated by any means with a child, meets with the child with the intention to commit any offence under the Act, is liable and can be punished with imprisonment for a term not exceeding 10 years and liable to whipping.

Sexting and Sextortion

Sexting is a combination of the words 'sex' and 'texting', where often the 'text' is sending an image or a video with or without a message. Sexting is defined as intentionally sharing of sexually explicit messages, images or videos using a mobile device or computer via the internet or chatting applications. These could be sexualised images of themselves that are 'self-generated' or forwarding sexualised images of others. These images or videos are often then shared with their peers.

Non-consensual sharing of self-generated sexually explicit material[7] is another form of sexting. Here the person may have shared a voluntarily produced sexual image with a friend but the trust is betrayed and the image then shared without consent with others.

Sextortion is a combination of the words 'sex' and 'extortion'. It is a form of online blackmail in which sexual information or images are used to coerce children into performing sexual acts for the perpetrator in which the act constitutes as sexual abuse. Often, these acts are being live streamed through devices or platforms where others watch remotely. As in all blackmail, the perpetrator will often demand more and more, and this may end up in a in-person meeting and physical sexual abuse. At times the sextortion is also used to generate financial or other personal gain.

[7] UNICEF. *What Works to Prevent Online and Offline Child Sexual Exploitation and Abuse? Review of national education strategies in East Asia and the Pacific 2020*.

Examples

As described above there are a number of forms of this type of online sexual abuse. The most common type that we encounter, for example, a young 12-14-year-old girl or boy who cultivates an online friendship with an individual who she/he thinks is a peer. As the relationship deepens, the adult perpetrator impersonating as a teenager, will either request for a nude or semi-nude image as 'an expression of love' or send one of their own to generate a response image from the child. Once the child sends a nude image, the whole relationship then changes and sextortion comes into full force. More and more demands are made of the child which then could escalate to rape or child sexual abuse material creation.

Other common occurrences are sexual images taken as part of physical sexual intimacy with a close friend (e.g. take a naked selfie together) but then betrayal happens. The presumed close friend now shares these images with others by peer-to-peer messaging apps or online. In this instance there may or may not be any sextortion since the perpetrator is a peer.

Motivation for Sharing Naked Images

The reason why children share sexually explicit images of themselves is not always easy to understand. Some children may be attracted to the other individual and want to share images as part of the 'deepening' relationship or in response to affirmative comments. Others may feel pressured by peers or pressured to maintain the relationship. At times there may be an element of experimentation and excitement in doing something 'dangerous'.

Finally, there is the adult perpetrator or a syndicate, often impersonating as a different person, who sexually grooms a child and then requests a sexual image as part of the relationship. Once one image is given, sextortion can be used in full force.

Impact

The consequences of sexting for a young person can be severe. They may experience humiliation and shame as the images are shared, especially with peers. Some peers may resort to harassing and bullying them in person or online. They may feel their reputation is irreversibly damaged and resort to self-harm and suicide.

Relevant Sections of the Laws

Sexual Offences Against Children Act 2017

Sexually communicating with a child (Section 11)
Section 11 prohibits any form of sexual communication with a child, except for education, scientific or medical purpose. Anyone found guilty is liable to imprisonment for a term not exceeding 3 years.

Non-physical sexual assault on a child (Section 15)
Section 15 prohibits any person from:

- Exposing a child to sexual words, sounds, gestures, objects, or body parts.
- Causing a child to display their body for sexual purposes.
- Repeatedly or persistently follows, watches, or contacts a child for sexual reasons.
- Engaging in sexual acts in the presence of a child, or causes a child to watch or hear sexual acts or sexual material in any form or medium.
- Causing or making a child participates in sexual activities.

Anyone found guilty is liable to imprisonment for a term not exceeding 10 years or fine not exceeding RM20,000 or both.

Sexual performance by a child (Section 15A)
Section 15A prohibits any involvement with a child in a sexual performance, including:

- Offering, procuring, or making a child available for a sexual performance.
- Making or causing a child to engage in a sexual performance.
- Participating in or viewing a child's sexual performance.
- Advertising, promoting, or facilitating a child's sexual performance.
- Receiving any benefit, including money, from a child's sexual performance

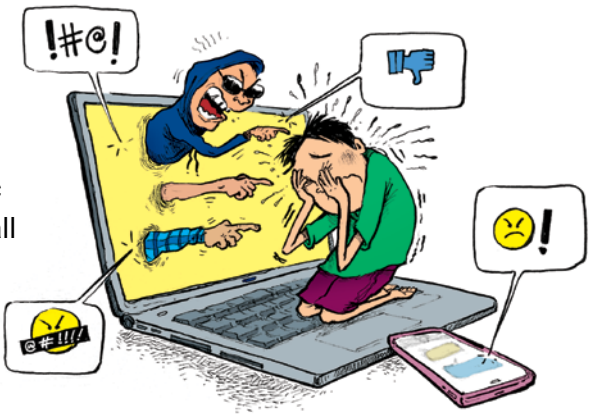
Anyone found guilty is liable to imprisonment for a term not exceeding 20 years and fine not exceeding RM50,000.

Sexual extortion of a child (Section 15B)
Section 15B prohibits anyone from:

- Threatening a child to engage in sexual activity.
- Threatening a child to share sexualised images, recordings, or representations of themselves, including genital, buttocks, breasts, pubic area, or anus, by any means.
- Threatening to distribute sexualised images, recordings, or representations of a child.

Anyone found guilty is liable to imprisonment for a term not exceeding 10 years.

Penal Code



Outrages on decency (Section 377D)
Section 377D prohibits any person from committing any act of gross indecency with another person, in public or private. If found guilty, the person shall be punished with imprisonment for a term which may extend to 2 years.

Inciting a child to an act of gross indecency (Section 377E)
Section 377E prohibits any person from inciting a child under the age of 14 years to any act of gross indecency with him or another person. Anyone found guilty is liable to imprisonment for a term of not less than 3 years and not more than 15 years, and also whipping.

Communications and Multimedia Act 1998

Prohibition of offensive content (Section 211)
Section 211 prohibits any service provider or any person to use the service provider to provide content which is indecent, obscene, false, menacing or grossly offensive with the intent to annoy, abuse, threaten or harass any person. Anyone found guilty is liable to imprisonment for a term not exceeding 10 year or fine not exceeding RM1 million or both and is also liable to a further fine of RM100,000 for every day or part of a day during which the offence is continued after the conviction.

Cyber-bullying and Doxxing

Cyber-bullying is bullying that is done through the use of technology, for example, using the internet or a mobile phone to hurt, harass, threaten or embarrass someone. About 50% of this kind of bullying is done by a person known to the child, like her/his classmate. Often the behaviour is repetitive and the child ends up experiencing anger, low self-esteem, anxiety and depression.

Doxxing comes from the word 'docs' as in 'documents'. It means to collect and share or 'publish' a person's private information online without their consent for the purpose of revealing their identity to others, causing many people to cyber-bully or cyber-harass them.

Examples

Cyber-bullying is common and a growing problem experienced in varying degrees by many children. A common example is someone who is jealous of a person, often a peer, who generates false information about them and spreads this online (often anonymously). This then has a 'life of its own' and escalates; at times with others joining in. The more the child tries to stop it, the stronger or louder the false messages become (called the 'Streisand effect').

This includes:

- Receiving mean, hurtful or threatening messages through social media platforms (e.g. Facebook, Instagram, Twitter, Snapchat, etc.) and messaging apps (e.g. WhatsApp, Telegram).
- Spreading rumours/lies about the child through social media platforms (e.g. Facebook, Instagram, Twitter, Snapchat, etc.) and messaging apps (e.g. WhatsApp, Telegram).
- Flaming, i.e. posting hostile or insulting comments on social media platforms to emotionally harm or elicit further responses from the child.
- Trolling the child, i.e. posting mean, hurtful or insulting messages online to upset her/him which can then lead to others joining in the bullying behaviour.
- Sending photos/videos of the child to others without the child's permission to embarrass, hurt or body shame her/him; or edit her/his images to embarrass her/him (e.g. sexual comments or edits).
- Excluding the child from chat groups or limiting her/his access to online conversations or comment posts.
- Online impersonation, i.e. people setting up fake profiles pretending to be the child or sending messages or posting status updates from her/his accounts.
- Account hijacking, i.e. hacking into the child's social media or other online profiles to change her/his information or control the profiles.

Motivation for Cyber-bullying

There are many reasons why some people become cyber-bullies. Some do so for revenge; some derive pleasure from seeing others suffer; some are bored or frustrated and use this as an outlet. Some cyber-bullies have been abused at home and take out their anger on others. Remember that children who are cyber-bullies also need our help.

Impact

Unlike physical bullying where the child usually knows the identity of her/his bully, in cyber-bullying it is often anonymous. This leads her/him to be suspicious of others and isolate themselves from her/his peers; the child does not know whom to trust. In addition, cyber-bullying has the potential to reach a wide audience and leave a permanent online record, making the impact on the victim more severe and longer lasting (recurring at times). Children experiencing cyber-bullying may feel fear, shame, humiliation, stress, and anxiety. They may also experience reduced school performance, become preoccupied with the bullying, social isolation, begin to avoid school and fall into depression. They often feel a sense of powerlessness and an inability to 'fix' things. Some may resort to self-harm and suicide.

Relevant Sections of the Laws

Communications and Multimedia Act 1998

Improper use of network facilities or network service (Section 233)

Section 233 prohibits misuse of network services. It is an offence to use any communication or network service to send messages that are obscene, indecent, false, menacing, or grossly offensive with intent to annoy, abuse, threaten, harass, or defraud, or to repeatedly send such messages.

Penalties:

- General offences: up to 2 years' imprisonment or fine up to RM500,000, plus RM5,000 per day if continued after conviction.
- Offences against a child (below 18 years): up to 5 years' imprisonment or fine up to RM500,000 or both, plus RM5,000 per day if continued.
- Obscene communications for commercial purposes: up to 5 years' imprisonment or fine up to RM1 million or both, plus RM10,000 per day if continued.

Cyber-stalking and Cyber-harassment

Cyber-stalking is the repeated use of electronic communications (over the internet) to stalk a child with the intention to harass or threaten her/him. This activity could target other groups of people. In cyber-harassment, the child is sent unwanted and negative messages, often repeatedly and frequently.

Examples

Remember that we may all receive a few negative comments on social media; this is not cyber-harassment. Only when the messages continue repeatedly over time and make us feel threatened, does it constitute cyber-harassment. Cyber-harassment can also take the form of 'text attacks' where a number of people gang up to send hundreds or thousands of messages to bully a child.

Cyber-stalking does not always involve direct communication with a child. A cyber stalker may stalk (i.e. follow and watch someone online over some time) a child without her/him being aware of the activity. The cyber-stalker may only act or interact with the child once they have amassed the data they require (personal details, account information, etc.). Online stalking may proceed to offline stalking and physical sexual abuse.

Note: Cyber stalker often use fake identities online.

Motivation for Cyber-stalking and Cyber-harassment

There are many possible reasons why an individual or group of people might do these activities. Some cyber-stalkers know their victims and may be motivated by anger and hurt (perceived past rejection), a desire to control the victims or sexual motives. Others may have a financial motive to blackmail someone or steal their identity (identity theft).

Impact

Children who have been cyber-stalked may have major psychosocial damage which includes fear, anger and depression. When it continues and does not appear to be able to be stopped, some children feel trapped, have suicidal thoughts and live increasingly isolated, anxious lives. Some end up with long term post-traumatic stress disorder (PTSD).

Relevant Sections of the Laws

Penal Code

Criminal intimidation (Section 503, 506 and 507)

Sections 503, 506 and 507 state that it is criminal intimidation if a person threatens another with any injury to this person, reputation or property with the intent to cause alarm to that person, even by an anonymous communication. Anyone found guilty of causing criminal intimidation is liable to imprisonment for a term which may extend to 2 years or fine or both. Anyone who commits criminal intimidation by an anonymous communication is liable to imprisonment which may extend to 2 years in addition to the punishment stated above.

Stalking (Section 507A)

Section 507A criminalises stalking, including cyber-stalking. This section prohibits a person from repeatedly harassing someone (at least twice) with the intent, or knowing it is likely, to cause distress, fear, or alarm to that person's safety. Harassment may include following or tracking someone, communicating or attempting to communicate in any way, loitering near their home or workplace, or sending or giving anything to the person. Upon conviction, any person is liable to imprisonment for a term not exceeding 3 years or fine or both.

Harassment, Threats, and Misuse of Identity Information (Sections 507B-507G)

Sections 507B-507G criminalise various forms of harassment, threats, stalking, cyber-stalking, and misuse of identity information, including conduct carried out online. These provisions prohibit the use of threatening, abusive, or insulting words, communications, or acts that cause or are likely to cause harassment, distress, fear, or alarm, making a person believe harm will occur, provoking self-harm, or facilitating harm. They also criminalise the publication or circulation of identity information (doxxing) to harass, intimidate, or endanger a person or their related persons. Punishments vary depending on the offence, ranging from fines and imprisonment of up to 1-3 years, with aggravated cases (such as those involving suicide or serious harm) carrying heavier penalties of up to 10 years' imprisonment.

Pornography

Pornography (often called 'porn') is the depicting or display of sexually explicit content either as images, videos or texts, for sexual arousal and pleasure of self or others. Children may be exposed to pornography unintentionally when surfing the internet or intentionally search for porn out of curiosity or heightened sexual desire at puberty. Pop-up adverts are a common source of sexual images. It is estimated that 10-20% of all online searches are for pornography. Some sections of pornography may normalise violence against women. Porn is searched for and looked at predominantly by men and boys.

Examples

Most children encounter pornography incidentally online or when a friend shares images or talks about looking at porn. Most children would have seen some pornography by the age of 12. Children hardly ever tell parents about online pornography as they know they will be scolded and their internet access restricted.

Impact

Early exposure to pornography creates misinterpretation of sexuality, relationships and the sex act among children. Pornography prioritises sexual gratification and downplays emotional connection which may lead children to perceive that relationship and sex are the same. Pornographic content creates unrealistic expectations about sex, negative self-perception regarding physical appearance and sexual functioning, and unhealthy intimate relationships.

It also often leads to a desire to see more explicit content and has a risk for pornography addiction. Addiction is primarily a repetitive brain reward that possibly works through a neurotransmitter called dopamine. Repetitive increase of dopamine due to watching pornography causes the brain to crave the same effect over and over again. Addiction to pornography may lead to earlier sexual experiences and unplanned pregnancies.

Child Sexual Abuse Material (CSAM)

The most disastrous and illegal aspect of pornography is online child sexual abuse material (CSAM). Children are exploited in the production of sexualised materials in a number of ways. The most common is by perpetrators taking images or videos of children and sharing them online.

There is also a large commercial element to such activities. Often children in poorer nations and communities are targeted to participate in image or video recordings, often performing sexual acts with adults, for money. There is a huge online traffic for images and videos of child sexual abuse. Much of this is hidden in the 'dark web'. Some prey on poor families and use online video applications to live-stream child sexual abuse materials. Increasingly we are seeing children, in financially difficult situations, sharing or selling their own sexual exploitation videos for financial gain.

There is a growing trend for peer-to-peer networks to share sexualised materials via mobile applications. This is also prevalent among older children. This sharing may include images or videos of friends that were shared consensually. Note that individuals that groom children for sexual purposes may use pornography as part of their activity.

Generative Artificial Intelligence[8]

Artificial intelligence (AI) has become increasingly widespread globally in recent years, with many tools now freely accessible. Much of society now relies on AI; whether to summarise a document, write an article, do school homework or generate an image. The quality of the AI image and video software has also grown exponentially. Currently images and videos can be produced with photorealistic quality. Generative AI is now being used in child sexual exploitation and abuse in many ways outlined below.

Examples

Image, Audio and Videos Manipulation: AI-generated or AI-altered media files, including image, audio and video materials are known as deepfakes. AI tools (such as 'nudify' apps) take original photos of children and digitally alter them to appear nude or engaged in sexual acts. Offenders can also use AI software to create new, hyper-realistic child sexual abuse material (CSAM) that does not involve real children. This content can be produced very quickly and on an enormous scale.

Revictimisation: Offenders can take existing CSAM and use AI to edit it, creating new versions of sexual abuse material involving known victims, thus further traumatising them.

Enhancing Online Grooming: Deepfakes, voice cloning and AI-powered tools have helped offenders to create fake child identities facilitating online grooming.

Generative AI has also increased the scope and impact of cyberbullying. Sadly, children themselves are increasingly becoming creators of AI-generated CSAM with devastating impact on their peers. There are also increasing reports of young persons deciding to have a relationship with an AI-generated individual or an AI application - this has the potential to degrade human relationships.

The threat of generative AI in online child sexual exploitation and abuse overshadows all other concerns. The wide accessibility of the tools lowers the barrier to entry for offenders and drastically increases the volume of CSAM online.

---

[8] *Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse*. Bracket Foundation in cooperation with the Centre for Artificial Intelligence and Robotics at the United Nations Interregional Crime and Justice Research Institute (UNICRI). https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf.

Impact

Even though AI-generated material is often artificial, the harm it creates is very real. Children, especially girls, whose likeness are used in AI-generated CSAM, suffer serious emotional harm, damage to their standing in society, inability to attend school and suffer social isolation. The lack of adequate measures to stop and remove online explicit deepfakes has led some teenagers to resort to self-harm. In addition, the mass production and distribution of AI-generated CSAM risks normalising abusive behaviours and attitudes toward the sexualisation of children.

Relevant Sections of the Laws

Sexual Offences Against Children Act 2017

Offences related to child sexual abuse material (Section 4 to 10)

Section 4 to 10 of the Act strictly prohibits the production, distribution, and viewing of child sexual abuse material. Child sexual abuse material is defined to cover all forms of visual, auditory, or written or combination of any means of a child or images of a child engaged in sexually explicit conduct.

It is an offence if a person:

- Makes, produces or directs the making of, or participates in any way, in any child sexual abuse material;
- Makes any preparation to make, produce or direct the making of, or production of any child sexual abuse material;
- Uses a child in making, producing, directing the making or production of any child sexual abuse material;
- Exchanges, publishes, etc., any child sexual abuse material;
- Sells, distributes, advertises, etc., any child sexual abuse material to a child;
- Accesses or has in possession or control of any child sexual abuse material.

Upon conviction, the person is liable to a fine, jail term and/or whipping.

Penal Code

Prohibition of selling, etc., of obscene materials (Section 292)

Section 292 prohibits any person from selling, distributing, producing, possessing, etc., any forms of obscene materials. The person shall be punished with imprisonment for a term which may extend to 3 years, or with fine, or with both.

Prohibition of selling, etc., of obscene materials to young person (Section 293)
Section 293 prohibits any person from selling, distributing, circulating, etc., obscene materials to any person under the age of 20. The person shall be punished with imprisonment for a term which may extend to 5 years, or with fine, or with both.

Prohibition of obscene acts or songs (Section 294)
It is an offence under section 294 if a person to the annoyance of others, does any obscene acts in any public places, sings, recites or utters any obscene song or words. The person shall be punished with imprisonment for a term which may extend to 3 months, or with fine, or with both.

Communications and Multimedia Act 1998

Improper use of network facilities or network service (Section 233)
Section 233 of the CMA criminalises the improper use of network facilities to transmit "*obscene, indecent, false, menacing or grossy offensive*" content. This gives authorities the power to act against individuals or platforms spreading digital CSAM.

Online Safety Act 2025

The Online Safety Act 2025 aims to promote and enhance online safety in Malaysia by regulating harmful content and providing for duties and obligations on applications service providers (ASPs), content applications service providers (CASPs) and network service providers.

The Act defines several categories of harmful content, including content on child sexual abuse material, financial fraud, and content that may cause harassment, distress, fear or alarm, incite violence or terrorism, or may induce a child to cause harm to himself. Of these, content on child sexual abuse material and financial fraud are defined as priority harmful content.

The Act also imposes several duties on ASPs and CASPs, including the duty to implement measures to mitigate users' risk of exposure to harmful content, make available a mechanism for reporting harmful content, to protect the online safety of child users, and to establish a mechanism for making priority harmful content inaccessible to all users.

3.0 What To Look Out For

This section outlines how we can recognise a child who is affected by online sexual abuse and steps to take.

Red Flags for Parents and Teachers: How to recognise if your child is affected online

Most children who are struggling online (sexually victimised or cyber-bullied) are unlikely to tell a teacher or parent. They may be afraid that the response from adults will be negative and punitive, feel embarrassed by what is happening, or concerned that their online privileges will be restricted or taken away. Hence it is important, as parents and teachers, to be alert to identify children who are affected.

Some of the key signs to suggest that they are having problems include:

1. **Nervous/Emotional when online** – Children who appear emotionally upset during or after using the Internet or when messages arrive.
2. **Secrecy** – Very secretive or protective of their digital life, hide or clear the screen when you enter their room or come near them.
3. **Social withdrawal** – Withdrawal from family, friends, or activities; avoiding school or social group gatherings.
4. **Marked changes in behaviour** – Unexplained behaviour change and/or a drop in academic performance.
5. **Mood swings** – Changes in mood, sleep, or appetite.
6. **Stop using** the computer or hand phone.

Not all children will respond in this way and some exhibit no sign that anything is wrong. Hence it is important to always have an open, two-way communication with any child in your care. Children tell us their concerns and worries when they trust us and know that we will not respond negatively and harshly.

What to Do When Things Go Wrong?

These are immediate steps and actions that a child can take:

1. **STOP** – Stop the communication with the perpetrator or bully and do not give in to any more demands.
2. **TELL** – Talk to a person she/he trusts like parents or a trusted adult (teacher, doctor).
3. **DOCUMENT** – Take screenshots and record all the communications. **Do not** delete these communications as they are important to keep as evidence.
4. **BLOCK** – Block the hand phone and online account of the perpetrator. At times she/he may need to get a new handphone number and email address.
5. **REPORT** – Get parents or a trusted adult's help to report the abuse to the relevant authorities (Refer to Handling Disclosure on page 25).
6. **PASSWORDS** – Change all her/his application and online accounts' passwords immediately and make them stronger.
7. **THERAPY** – Get her/him professional help from a counsellor to work through her/his trauma.

4.0 Handling Disclosure[9]

Children need to be trained in two areas:

Keep No Secrets
Instruct children to always tell a trusted adult (parent, teacher or doctor) if they are uncomfortable about anything that has happened online, including the behaviour of another person towards them. This applies even if the child feels they have done something wrong.

The Right to Say No
Every child must understand that she/he has the right to say no to any kind of communication that she/he does not like. She/he should tell the carer or teacher about any inappropriate communication with someone that feels wrong.

Principles for disclosure

a. Always maintain strict confidentiality for the child. Do not gossip about the problem to others. Do not disclose the child's identity in any way to the media.

b. Inform the child's parents that you suspect abuse. Parents do not have the right to refuse notification or any intervention for the child.

c. Continue to support the child or find an appropriate person who can do so. The child might need specialised help or counselling.

[9] Amar-Singh HSS (2019). *Child Safe Programme*. National Evangelical Christian Fellowship (NECF).

Talking to Children

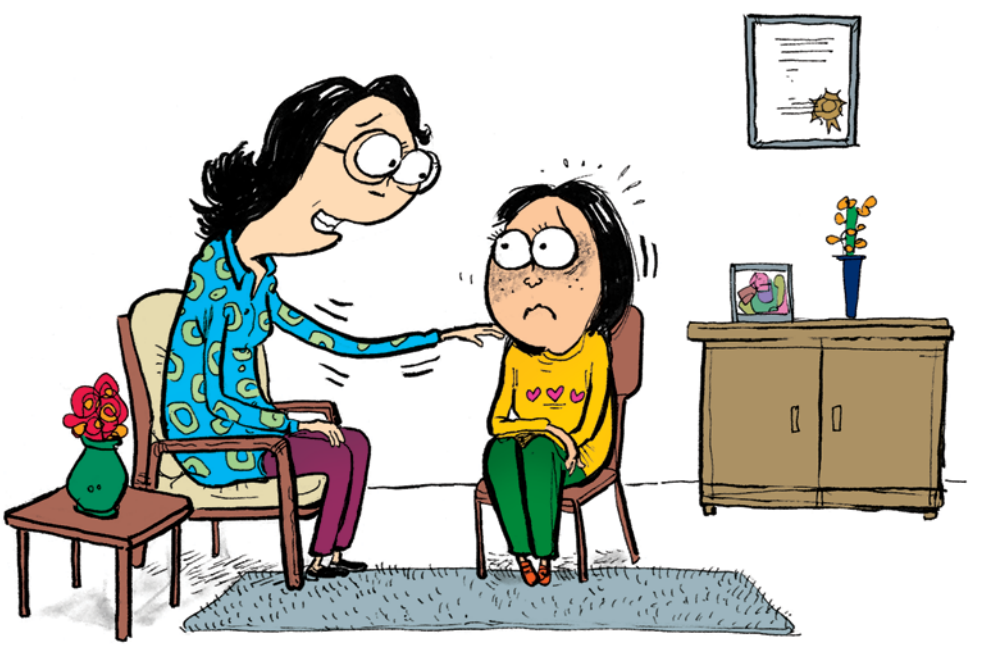
Supporting children is not always easy and will require parents and teachers to have empathy, a listening approach and be age appropriate. Here are some guidelines:

1. It is best to have a safe, private place to have a conversation with the child. If possible, have a chaperone or at least an open door or glass window in the door to avoid any risks or misunderstanding.

2. Communicate in an age appropriate manner. Use simple, clear words when communicating but do not talk down to the child. Listening to the child and offering her/him an opportunity to express her/his concerns is vital. Avoid any judgemental outlooks verbally or in facial expressions.

3. Reassure the child that you will maintain confidentiality but state clearly that this will not happen if the child is being harmed or is planning to harm others. When the child shares experiences of being abused, express that you believe her/him and that it is not her/his fault.

4. While we would like to tell children that they will be kept safe and will be protected from further abuse, this is not always possible to achieve. Tell them that you will try your best to improve their situation. We should always act in the best interest of the child.



Report Procedures

All forms of online sexual abuse of children must be reported. This is a legal requirement under the Child Act 2001 (revised 2016) and Sexual Offences Against Children Act 2017. A parent or teacher must never hide or ignore a child's concerns or disclosure about abuse. If a child tells the parent or teacher about it, it is important to listen, take it seriously and report it (or seek help for an evaluation). There are two types of reporting as described below:

A. When the Abuse Happens Online

1. Tell a trusted adult about it

Encourage the child who experienced any online sexual abuse or problems to discuss it with a person she/he trusts like parents or other trusted adults (e.g. teacher, doctor). We should let the child know that not all secrets should be kept, especially if she/he is being harmed. Adults should, as a first step, enable the child to stop all further communication with the abuser and not to give in to any more demands. It is important if the child tells another adult, the parents are also informed.

2. Keep evidence of the online sexual abuse

It is vital to document all the communications that have taken place online. Record all the communications by taking screenshots (preferably time-stamped) and saving them both digitally as well as printing hard copies. Do not delete these online communications as these are important evidence.

3. Block and cut off all communication with the abuser

Block the phone number and online account of the perpetrator. This includes blocking the person on all social media platforms. At times you may need to get the child a new phone number and new email address. If significant sexual shaming has happened online (widespread) then the child may want to stop going online and start afresh later with a new profile. Also change the passwords for all handphone applications and social media accounts immediately and make them stronger. It may be useful to install some anti-malware software and scan the phone and computer.

4. Make a police report

Accompany the child and parents to the local police station to make a formal report. Prepare the family before they make the report. Bring hard copies of all the evidence.

Facts required in a police report on online violence

- **WHEN:** When did it occur? Date and time of the incident(s).
- **WHICH:** Which online platform(s)?
- **WHO:** Who was involved? The identity or description of suspect.
- **WHAT:** What was the incident? Details of the incident(s).
- **HOW:** How did it happen and how many times?
- **EFFECT:** What's the effect on you after the incident? Damages, losses or any injury sustained, depression, fear, etc.
- **WHY:** Why is the report being lodged? To take action, for safety, etc.

SAMPLE OF A POLICE REPORT

On _____ (date and time), I befriended a person named _____ (name or other details) through _____ (online platform). On _____ (date and time), I received _____ (what incident) in my _____ (online platform) from the person. The person threatens to spread them into other social media applications if I do not meet him/her in person. This incident happened _____ (how many times). I am scared for my safety and experiencing _____ (effect).

The reason I make the report is for the authorities to take action.

5. Make a report to Malaysian Communications & Multimedia Commission

Malaysian Communications & Multimedia Commission (MCMC)

- Hotline (office hours only): 1800-188-030
- E-mail: aduanskmm@mcmc.gov.my
- Online Complaint: https://aduan.skmm.gov.my
- Submit your police report when you lodge a complaint.

6. Consider therapy for the child

Some children who have been seriously traumatised may require professional help from a counsellor to work through the trauma. Many suffer from post-traumatic stress disorder (PTSD).

B. When the Online Abuse Becomes Physical Abuse

When the online abuse becomes physical sexual abuse, the child should be taken to one of the following agencies: government hospital, Social Welfare Department (*Jabatan Kebajikan Masyarakat, JKM*) or police. There may be non-governmental organisations (NGOs) in your area that are active in child protection work and can help the child and family through this whole process; like offering counselling, interagency liaison and support their court trials.

The following table will give you an idea of what happens to a sexually abused child when she/he is taken to these agencies and offer guidance on how to deal with the visits.

*Note: The procedure at each government hospital may vary, especially at the larger hospitals that have Paediatric Departments. A summary of what to expect is outlined as follows:

Getting Admitted	There are two possible options. Some hospitals prefer all children to go through the One Stop Crisis Centre (OSCC) of the Emergency Department. Other Paediatric Departments prefer seeing children in the clinic or straight away (after hours) and admit them directly to the ward. Admission for children will usually be in the paediatric wards but older girls may be warded in the obstetrics and gynaecology ward and older boys in the surgical ward.
Necessity for a Police Report	All government doctors are required by law (Child Act 2001) to take a suspected abused child into protection even if a police report has not been lodged. The police report is required to help with investigations, authorise the medical examination and allow for samples to be used in court proceedings. The police report can be made by the parents, government doctors or Social Welfare Department (JKM) staff. Many bigger hospitals have a police counter at the Emergency Department. Even if a police report is withdrawn by the parents, the doctors are obliged by law to act and notify JKM.
Examination	Examination will take place either in the OSCC of the Emergency Department or in the Paediatric ward. Many larger government hospitals with Paediatric Departments will have a Suspected Child Abuse and Neglect (SCAN) Team to oversee the process. Examination is often done jointly by the Paediatrician and the Gynaecologist. The police will be required to be available to receive samples and maintain the chain of evidence.
Notification of and Role of JKM	JKM will be notified (in writing) by the Paediatric Department as soon as the child is admitted. The JKM officer will come to interview the child, parents/guardian and doctors in charge of the case.
Discharge and Counselling	While the child is in the hospital, she/he will receive medical attention and counselling. The decision to go home is made jointly between the Paediatric Department and JKM. The key issue will be to ensure the child is placed in a safe environment.

Role of Police	The police will investigate the complaint and collect evidence for the prosecution of the suspect. Once a police report has been lodged, an Investigating Officer (IO) will then be assigned to take on the case for further investigation, which includes taking statements from the child, doctors involved and the suspect. Once the investigation is completed, the IO will submit a report to the Deputy Public Prosecutor (DPP) who will then determine whether the case can be brought to court. Note: In many of the cases, the DPP may make a decision not to charge the suspect in court if there is insufficient evidence.

Facts required in a police report on physical sexual assault

- **WHEN:** When did it occur? Date and time of the incident(s).
- **WHERE:** Where did it happen? Location(s).
- **WHO:** Who was involved and who was the alleged perpetrator?
- **WHAT:** What was the incident? Details of the incident(s).
- **HOW:** How did it happen and how many times?
- **EFFECT:** What's the effect on the child after the incident? Bruises, injury, depression, fear, etc.
- **WHY:** Why is the report being lodged? To take action, for safety, etc.

SAMPLE OF A POLICE REPORT

On _____ (date and time), when I was at _____ (address/location), I was raped by _____ (name or other details of perpetrator). The perpetrator forced _____ (details of the incident). I had befriended the perpetrator _____ (name or other details) through _____ (which online platform) since _____ (when). The rape happened _____ (how many times) on/at _____ (date and time/previous locations). Due to the rape, I suffered _____ (effects).

The reason I make the report is for the authorities to take action.

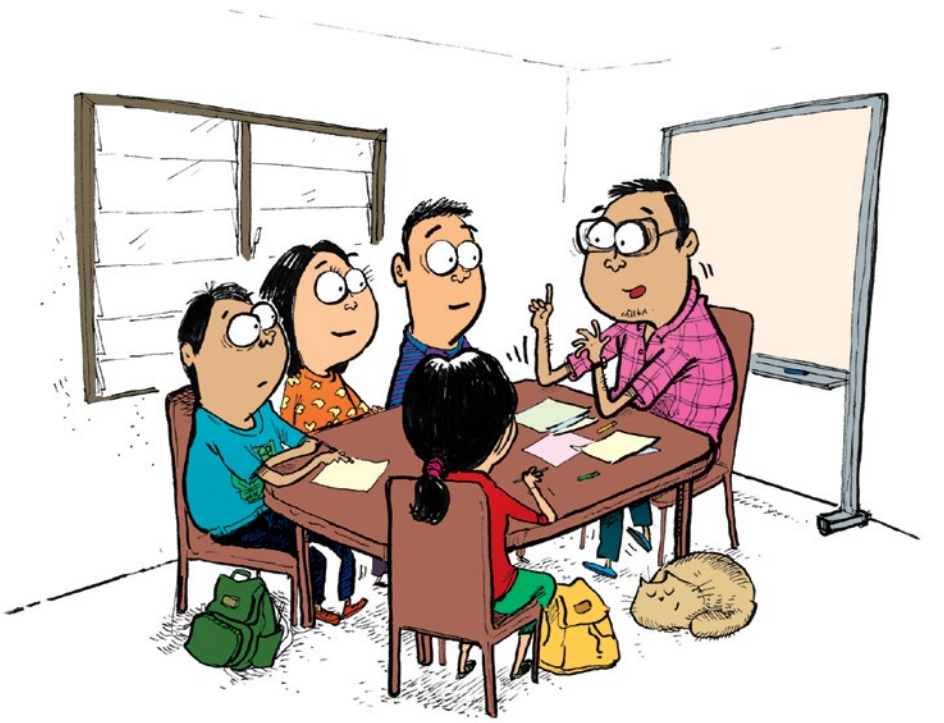
5.0 Activities

This section discusses the different types of online sexual abuse and offers activities for each of them. Most activities require about 45 to 60 minutes to complete and are best done with a group of participants. Each type of abuse is discussed using a case study or/and an activity.

Rather than conducting this in a formal style, it is recommended that participants be divided into smaller groups of 5-7 persons and be asked to offer opinions and suggestions for each situation. This will allow for more interactive learning. Each activity comes with a worksheet that can be given out to each small group of participants to facilitate discussion.

The activities can be conducted with participants aged 12-18 years. Younger participants aged 9-11 years may also benefit from the sessions but the activities will have to be adapted and made simpler for their use.

Educators and facilitators are recommended to continuously source updated and relevant videos on cybersafety to work with participants.



Topic 1: The Friends We Have

Activity - Circle of Friendship[10,11]

Circle of friendship or social circles is a graphic way of showing participants the different levels of familiarity they have with people they know and don't know. It is an activity which helps participants explore the different types of friends they have including online friends. The activity also helps them discuss the issue of trust and sharing of information with different types of friends through the 'Circle of Friendship' diagram.

Learning Objectives

- To differentiate different categories of friends (close, casual, acquaintance and online friends).
- To know who one can trust and how to create safe boundaries in relationships.

Time Required: 45-60 minutes

Materials

- A white board to record answers and responses.
- Some paper to write on.
- A4 paper with 'Circle of Friendship' diagram, mahjong paper, marker pens, blue-tack.

Methodology

1. Inform the participants about the learning objectives.
2. Divide the participants into groups of 5-7 persons and make sure that each one has a copy of the A4 paper with a 'Circle of Friendship' diagram.
3. Ask each participant to write their name in the central circle (and/or paste her/his picture there). Explain to her/him this is their personal space, her/his body, and that only certain people can get very close to her/him.
4. On the next circle ask them to write "friends". At this point ask the participants why they have friends and to describe the characteristics of a good friend. List their answers on the white board and ask them to reflect and select what they think are the most important characteristics. From their feedback, highlight trust as an important characteristic.

---

[10] Amar-Singh HSS (2019). *Child Safe Programme*. National Evangelical Christian Fellowship (NECF).

[11] Hasanah Akhir, Hana Husni, Prema Devaraj (2017). *Cybersafety Programme for adolescents 12 to 17 years: Guidelines for facilitators and trainers*. Women's Centre for Change, Penang.

5. Discuss the different types of friends they have and explain the differences.
   a. **Close friend:** someone whom you know very well and who knows you well; someone you might give a hug to, consider a special friend and share your secrets.
   b. **Casual friend:** someone whom you know a little better and have an occasional chat with.
   c. **Acquaintance:** someone you know just casually in your neighbourhood or school and might say a polite hello to.
   d. **Online friend:** someone you just met online and you have not known them in-person.

6. Ask the participants to discuss the differences in the activities they would engage in with acquaintances and with close friends e.g. sharing secrets with a close friend but not with a casual friend or an acquaintance.

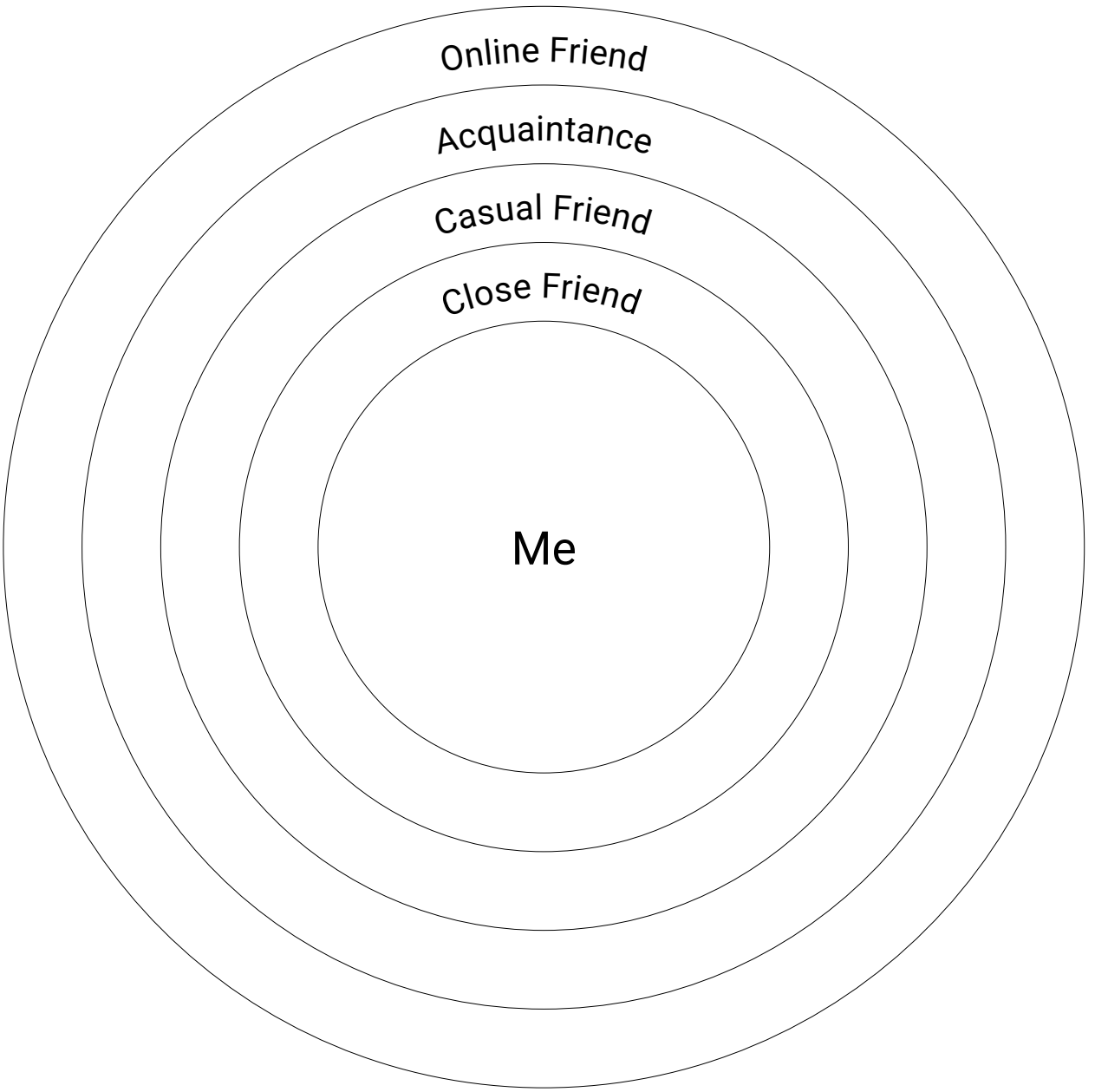
7. Discuss how we can build trust and that it takes time and experience for this to happen.

8. Ask them whether or not they can trust the friends they have made online. Get them to explain why.

9. Lastly, on the outside of the last circle ask them to write "strangers" i.e. people you don't know. Teach them to ignore these people and not allow them to touch you.

10. Use different colours for each circle (red for the outer-most to designate danger) to help clarify its meaning to the child. Remember that visual cues like these are a great way to backup verbal communication.

Worksheet: Circle of Friendship



Topic 2: Online Grooming of Children for Sexual Purposes

Activity: Two Case Studies (Amelia's Story and Ethan's Story)

Learning Objectives

- To understand what "Online Grooming of Children" is and to be able to identify if it is happening.
- To have a better insight on the reliability and safety of an online 'friend' and how to develop good online interactions.

Time Required: 45 minutes

Materials

- A white board to record answers and responses.
- Some paper to write on.
- Projector to share one case study and questions or print the case study and questions as handouts for the participants – use the worksheet provided (Do not give the answers to the students until they have provided theirs). Refer to the Discussion Points on pages 38-39.

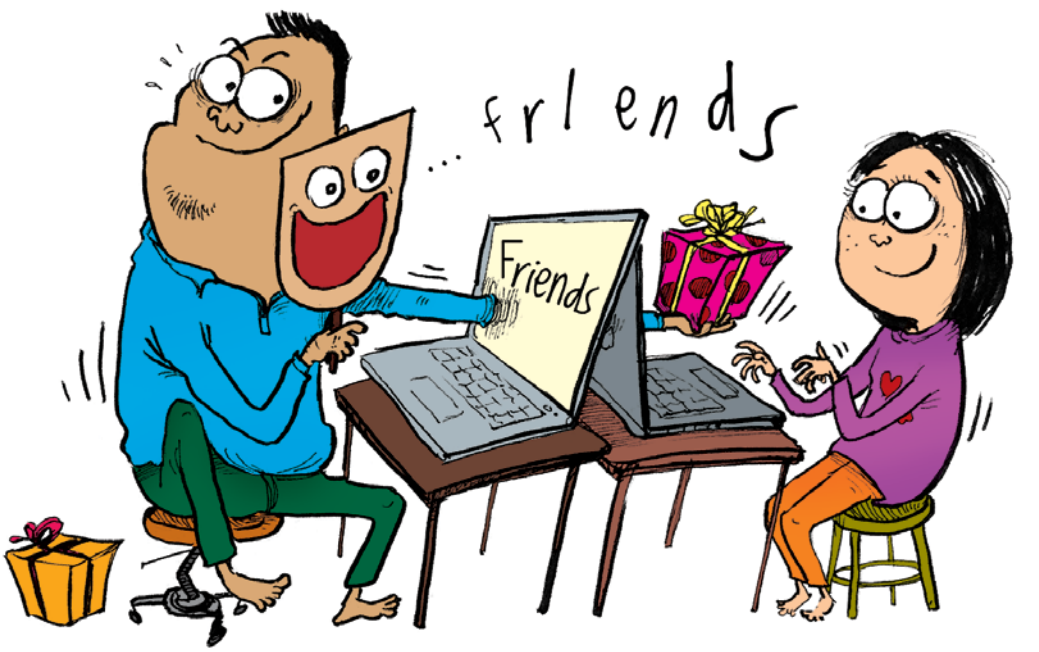
Methodology

1. Inform the participants about the learning objectives.
2. Divide the participants into groups of 5-7 persons.
3. Start by sharing what is 'Online Grooming of Children for Sexual Purposes' (Refer to page 7).
4. Read the case study out loud and share a worksheet with each group. Note that there are 2 case studies – one girl (Amelia's story) and another boy (Ethan's story). You can do both or only choose one.
5. Ask the participants to discuss and note down their answers.
6. Get the groups to respond to the questions (to save time, each group can answer one question and others can offer different opinions if any).
7. Discuss 'How Online Groomers Work' (Refer to page 8).
8. Consider giving a copy of the 'Red Flags' (refer to Appendix 1) to each participant to put up in their bedroom or location where they often access the internet.

Case Study 1: Amelia's Story

Amelia is a 13-year-old girl and she was bullied in school. The bullying affected her self-esteem and made her feel vulnerable. Struggling to make friends in school, she turned to online gaming. Soon, she befriended an online gamer, Alfie, who was understanding and knowledgeable. They began chatting for hours, usually at night, and soon started exchanging messages on Discord (an app for gaming and socialising). They expressed how much they liked each other. Alfie asked Amelia to be his girlfriend, and Amelia happily agreed to it.

Alfie started requesting photos of Amelia, eventually asking for naked images. Amelia felt uneasy about sending such pictures, but she liked Alfie a lot and did not want to disappoint him. Alfie comforted her, saying that these photos will be safe with him. He also reassured her that this is common for couples who are in a romantic relationship. Although Amelia hesitated, she eventually decided to send her photos. One day, Amelia's friend told her that her images had gone viral and were being sold. Amelia was so shocked and did not know what to do.



Case Study 2: Ethan's Story

Ethan is a 12-year-old boy who is quiet and shy. He has hardly any friends at school. His parents also have two younger children aged 2 and 4. Much of the parents' time is spent looking after the younger children. Ethan turned to using online chat groups more as a means to try and find some friends and companionship. He was befriended by a girl named Sarah who was about his age. Over some months they developed a relationship and gradually communicated more and more; initially on social media sites and then one-to-one using WhatsApp. Sarah said she was delighted to have 'found' Ethan and that he may be her soul mate. They exchanged many personal images of each other; some images Sarah sent were seductive.

One day she sent him a picture of herself half naked and asked him to respond. Ethan sent her a picture of himself showing his genitalia. The relationship then changed rapidly. Ethan had a video call from 'Sarah' and found out 'she' was an older adult man. Ethan was terrified. The man said he would share his naked images with all his classmates at school unless Ethan does all that he asked. Ethan's behaviour at home and school changed. He became even more of a loner but his parents and teachers did not notice this. One day the man demanded Ethan meet him at his flat. Ethan went and was sexually abused.

Discussion Points

1. **What are the characteristics of a good friend; someone whom you can trust?**

   - Good friends will respect you and your values.
   - Friends will listen to your points of view and be prepared to admit if they are wrong.
   - Reliable friends are trustworthy and keep your confidences (secrets) and will not use them to blackmail you.
   - Dependable friends will be there for you through bad and good times.
   - True friends will apologise if they hurt you and not repeat it.
   - Will never ask or pressure you to do something wrong.
   - Will not send or ask for sexual images.

   Basically, we should expect the same values in online relationship and face-to-face relationship.

2. How can you know the person (stranger) you meet online is a safe person?

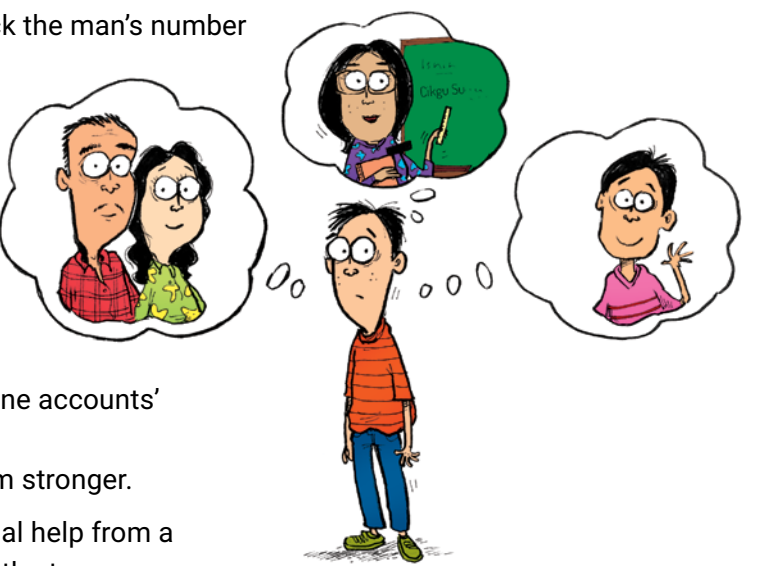
This is very difficult to answer and requires insight, intuition and experience. You need to be alert of red flags (warning signs) when the online person:

- Praises you a lot, especially your appearance ('you look so pretty or handsome').
- Tries and moves the relationship/communication to a private one (one-to-one).
- Asks you to keep the relationship secret.
- Inquisitive about your personal life and asks for information (e.g. address, hand phone number, etc.).
- Wants to send you gifts.
- Wants to meet face-to-face or asks you for an intimate photograph.

The important point is to always take time to develop the relationship and to do this in an open platform or in a group. This same principle applies to physical relationships as well. When in doubt or if the child feels uncomfortable, always talk about the relationship to a person she/he trusts like parents or a trusted adult.

3. What should Amelia/Ethan do now in this difficult situation?

- **STOP** – Stop the online and physical meetings with the man and not give in to any more demands.
- **TELL** – Talk to a person she/he trusts like parents or a trusted adult (teacher, doctor).
- **DOCUMENT** – Take screenshots and record all the communications. **Do not** delete these communications as they are important to document as evidence.
- **REPORT and BLOCK** – Block the man's number and account online and get parents' help to report the abuse to the relevant authorities (Refer to Appendix 3: Useful Contacts on pages 77-84).



- **PASSWORDS** – Change all her/his application and online accounts' passwords immediately and make them stronger.
- **THERAPY** – Get professional help from a counsellor to work through the trauma.

Worksheet: Grooming of Children for Sexual Purposes

Case Study: Amelia's Story

Amelia is a 13-year-old girl and she was bullied in school. The bullying affected her self-esteem and made her feel vulnerable. Struggling to make friends in school, she turned to online gaming. Soon, she befriended an online gamer, Alfie, who was understanding and knowledgeable. They began chatting for hours, usually at night, and soon started exchanging messages on Discord (an app for gaming and socialising). They expressed how much they liked each other. Alfie asked Amelia to be his girlfriend, and Amelia happily agreed to it.

Alfie started requesting photos of Amelia, eventually asking for naked images. Amelia felt uneasy about sending such pictures, but she liked Alfie a lot and did not want to disappoint him. Alfie comforted her, saying that these photos will be safe with him. He also reassured her that this is common for couples who are in a romantic relationship. Although Amelia hesitated, she eventually decided to send her photos. One day, Amelia's friend told her that her images had gone viral and were being sold. Amelia was so shocked and did not know what to do.

Discussion

1. What are the characteristics of a good friend; someone whom you can trust?

2. How can you know the person (stranger) you meet online is a safe person?

3. What should Amelia do in this difficult situation?

Worksheet: Grooming of Children for Sexual Purposes

Case Study: Ethan's Story

Ethan is a 12-year-old boy who is quiet and shy. He has hardly any friends at school. His parents also have two younger children aged 2 and 4. Much of the parents' time is spent looking after the younger children. Ethan turned to using online chat groups more as a means to try and find some friends and companionship. He was befriended by a girl named Sarah who was about his age. Over some months they developed a relationship and gradually communicated more and more; initially on social media sites and then one-to-one using WhatsApp. Sarah said she was delighted to have 'found' Ethan and that he may be her soul mate. They exchanged many personal images of each other; some images Sarah sent were seductive.

One day she sent him a picture of herself half naked and asked him to respond. Ethan sent her a picture of himself showing his genitalia. The relationship then changed rapidly. Ethan had a video call from 'Sarah' and found out 'she' was an older adult man. Ethan was terrified. The man said he would share his naked images with all his classmates at school unless Ethan does all that he asked. Ethan's behaviour at home and school changed. He became even more of a loner but his parents and teachers did not notice this. One day the man demanded Ethan meet him at his flat. Ethan went and was sexually abused.

Discussion

1. What are the characteristics of a good friend; someone whom you can trust?

2. How can you know the person (stranger) you meet online is a safe person?

3. What should Ethan do now in this difficult situation?

Topic 3: Sexting and Sextortion

Activity 1: Online Dangers in Chat Apps

Scan QR

Scan QR

Learning Objectives

- To highlight the dangers of using chat applications when making friends.
- To raise awareness on avenues for help.

Time Required: 45 minutes

Materials

- WCC Cybersafety YouTube video *Chat Apps* and *Cyber Violence? Beware, Be Safe*.
- Laptop, sound speakers, projector, mahjong paper and marker pens.

Methodology

1. Gather all the participants together.
2. Next, ask the participants what type of chat apps they use or know of.
3. Ask the participants why people use chat apps.
4. Ask the participants to show how well they know their chat app friends, i.e. can they be trusted? (Refer to Topic 1 'The Friends We Have' on page 33)
5. Invite two of the participants to role play Scenario A and another two persons to play Scenario B below (Select different genders to do role play).

   Scenario A: Hanging out in-person
   You're hanging out alone at a cafe. A stranger approaches you to get acquainted. What would you do?

   Notes to Facilitator

   - Invite two volunteers from the group to role play a child and a stranger.
   - Encourage the participants to act the scenario without any judgemental comments.
   - After the role play, ask them the following questions:
     a) How do you feel when approached by a stranger?
     b) Did you provide your personal information to the person?
     c) Why did you behave in such a way?
   - Write the answers given by the participants on mahjong paper.

Scenario B: Chat Apps
(Example: WhatsApp / Telegram)
You receive a random test from someone you do not know on WhatsApp. What would you do?

Notes to Facilitator

- Invite two volunteers from the group to role play a child and a stranger.
- Encourage the participants to act the scenario without any judgement comments.
- After the role play, ask them the following questions:
  a) How do you feel when you receive a random test from a stranger?
  b) Will you respond to the text? If so, what are your criteria for responding request?
  c) Is it different from the way you make friends in-person? If so, why?
  d) Which category does this friend belong to?
- Write the answers given by the participants on mahjong paper.

6. Tell the participants you are going to show them a video about chat apps and that after watching the video there will be a discussion.

7. Play the WCC Cybersafety video *Chat Apps* (https://youtu.be/VLXhW4vn0wQ). At the end of the video, get them to express what they understand from the video. (They should be able to summarise what they saw). As the video is short, it might be necessary to play the video again.

Scan QR

8. Ensure that they understand that not all online friends are trustworthy. Some might be sexual predators.

9. Ask the participants what they should do if something like this were to happen to them or their friends.

10. Once they have explored some options, play the WCC Video *Cyber Violence? Beware, Be Safe* (https://youtu.be/oUxbggKtQN8)

Scan QR

11. Explain to the participants that it is generally okay to make friends but they must be careful who their online friends are.

Activity 2: Video *Kisah Lila*

Learning Objectives

- To raise awareness on the dangers of sexting.
- To be aware of where to seek help.

Time Required: 45 minutes

Materials

- WCC Cybersafety YouTube video *Kisah Lila* and *Cyber Violence? Beware, Be Safe*.
- Laptop, sound speakers, projector, mahjong paper and marker pens.

Scan QR Scan QR

Methodology

1. Gather participants together.
2. Next ask the participants what they understand by the term "sexting".
3. Then explain what sexting is.
   Sexting *is the sending, receiving, or forwarding of sexually explicit messages, images or videos, primarily between mobile phones. It may also include the use of a computer or any digital device.*
4. Ask them why they think people engage in sexting.
5. Tell them you are going to show a video about sexting and that after the video there will be a discussion.
6. Play the WCC Cybersafety video *Kisah Lila* (https://youtu.be/OjyGFlJWQdA). At the end of the video, get them to express what they understand from the video. (Participants should be able to summarise what they saw). As the video is short, it might be necessary to play the video again.

Scan QR

7. At the end of the video, get the participants to tell you what the video was about.
8. Next ask the participants the following questions:
   a) Why did the boyfriend ask for Lila's photo?
   b) Why did Lila send the photo?
   c) Why did the boyfriend forward Lila's picture to his friends?
   d) What do you think how Lila felt when she found out?
   e) What do you think Lila can do about the situation?
   f) Where do you think Lila can seek help?

9. Once they have explored options on where they can seek help, play the WCC Cybersafety video *Cyber Violence? Beware, Be Safe* (https://youtu.be/ oUxbggKtQN8).

10. Explain to the participants that while it is quite normal to take and share photos with their family and friends, they need to be very cautious about the type of photos they take (i.e. nothing explicit) and with whom they share their photos. If they do not really know or trust a person, they should not share any photos with them. Emphasise that once they share a photo, they lose control over what will happen to that photo.
11. Highlight to the participants that any photos or media that are sent out can be circulated and posted online. **Remind them: Digital footprint stays forever. Think twice before you act.**

Activity 3: Case Study (Nora's Story)

Learning Objectives

- To understand what sexting is.
- To become aware of risks and consequences of sharing sexually explicit images or selfies.
- To know how to respond when receiving sexual materials and requests for sexual images of yourself.

Time Required: 45 minutes

Materials

- A white board to record answers and responses.
- Some paper to write on.
- Projector to share the case study and questions or printed handouts – use the worksheet provided (Do not give the answers to the students until they have provided theirs). Refer to the Discussion Points on pages 46-47.

Methodology

1. Inform the participants about the learning objectives.
2. Divide the participants into groups of 5-7 persons.
3. Start by sharing what is Sexting and Sextortion with the participants (Refer to page 10).
4. Read the case study (Nora's story) out loud and share a worksheet with each group.

5. Ask the students to discuss and note down their answers.
6. Get the groups to respond to the questions (to save time, each group can answer one question and others can offer different opinions if any).
7. Discuss what we can learn from Nora's story.
8. Discuss the motivation for sharing naked images and consequences of sexting (Use the Discussion Points on Nora's story below).

Case Study: Nora's Story

Nora is a 14-year-old girl, the only child of parents who are both successful and busy professionals. She is active on social media, especially Instagram. A week ago, she befriended a boy named Adam online and their relationship developed quickly. He was kind, attentive, listened to her and often praised her, especially her looks. She felt very much appreciated and she was in love with him. He then asked her for a naked picture of her body, so that he could admire her further. He expressed hurt when she was initially reluctant to give it. He promised that only he would see it and no one else would have access to the image. She was worried he would break off the relationship if she did not agree, so she sent him one naked image of herself.

The relationship changed after this. She found out he was actually an adult man. He now threatens her to expose and share her picture online with others, her parents and friends unless she sends him even more images. She felt so trapped and frightened so she sent more images. He then asks her to video chat with him and exposes her body to him, as well as do sexual things he instructs her to do to her body. He records this video call. She is now depressed and has thoughts of ending her life.

Discussion Points

1. Why did Nora send a nude image to Adam?

- She felt liked and appreciated by Adam.
- She was afraid that he might break off the relationship.
- She trusted his promise that he would not share it.
- She assumed his online profile was genuine.

2. How should Nora have responded when she was pressed for a nude image?

- She can be firm and trust herself and not send one (inner voice).
- She can try to speak to her parents about the request (she probably may not do this as she did not want them to know about the relationship).

3. What should Nora do now in her difficult situation?

- **STOP** – Stop the communication with Adam and do not give in to any more demands.
- **TELL** – Talk to a person she trusts like parents or a trusted adult (teacher, doctor).
- **DOCUMENT** – Take screenshots and record all the communications. **Do not** delete these communications as they are important to keep as evidence.
- **REPORT and BLOCK** – Block Adam's number and account online and get parents' help to report the abuse to the relevant authorities (Refer to Appendix 3: Useful Contacts on pages 77-84).
- **PASSWORDS** – Change all her application and online accounts' passwords immediately and make them stronger.
- **THERAPY** – Get professional help from a counsellor to work through the trauma.

4. What can we learn from Nora's story?

- It is OK to say 'NO' when someone asks for sexually explicit images.
- People who love us will respect our bodies and personal space/values.
- It is OK to break off a relationship or block a person who persistently asks you for sexual images.
- Never keep these kinds of harmful secrets.
- The earlier you tell your parents or a trusted adult, the smaller the damage will be.

5. Additional reflective questions

- How would you react if you saw a naked photo of your friend or classmate online?
- What would you do if someone sent you a naked photo of another person?
- How would you feel if you found out your boyfriend or girlfriend shared naked pictures of you with others?

Worksheet: Sexting

Case Study: Nora's Story

Nora is a 14-year-old girl, the only child of parents who are both successful and busy professionals. She is active on social media, especially Instagram. A week ago, she befriended a boy named Adam online and their relationship developed quickly. He was kind, attentive, listened to her and often praised her, especially her looks. She felt very much appreciated and she was in love with him. He then asked her for a naked picture of her body, so that he could admire her further. He expressed hurt when she was initially reluctant to give it. He promised that only he would see it and no one else would have access to the image. She was worried he would break off the relationship if she did not agree, so she sent him one naked image of herself.

The relationship changed after this. She found out he was actually an adult man. He now threatens her to expose her and to share her picture online with others, her parents and friends unless she sends him even more images. She felt so trapped and frightened so she sends more images. He then asks her to video chat with him and exposes her body to him, as well as do sexual things he instructs her to do to her body. He records this video call. She is now depressed and has thoughts of ending her life.

Discussion

1. Why did Nora send a nude image to Adam?

2. How should Nora have responded when she was pressed for a nude image?

3. What should Nora do now in her difficult situation?

Topic 4: Cyber-bullying and Doxxing

Activity 1: Cyber-bullying

Learning Objectives

- To understand and stop cyber-bullying.
- To be aware of the impact of cyber-bullying on children.
- To speak out against cyber-bullying.

Time Required: 45 minutes

Materials

- WCC Cybersafety YouTube video *Cyber-bully* and *Cyber Violence? Beware, Be Safe*.
- Laptop, sound speakers, projector, mahjong paper and marker pens.

Scan QR Scan QR

Methodology

1. Gather the participants together.
2. Next ask the participants what they understand by the term "bullying". Ask them to give examples of bullying they are aware of either in school or elsewhere.
3. Ask them why they think bullying takes place.
4. Then explain what cyber-bullying is.
   Cyber-bullying *is bullying that takes place online and/or by using digital devices like handphones, computers, and tablets. It can happen through chat applications, social media, forums, or gaming platforms. In other words, it can happen where people can view, participate in, or share content.*
5. Tell the participants you are going to show them a video about cyber-bullying and after that there will be a discussion.
6. Play the WCC Cybersafety video *Cyber-bully* (https://youtu.be/XPf8T-zFhu8). At the end of the video, get them to express what they understand from the video. (Participants should be able to summarise what they saw). As the video is short, it might be necessary to play the video again.

   Scan QR
7. Next ask the participants the following questions:
   a) How do you think the victims of cyber-bullying feel?
   b) Now that you know, do you think bullying is ok?
   c) What can you do if you know someone is being bullied?

8. Once they have explored options on where they can seek help, play the WCC Cybersafety video *Cyber Violence? Beware, Be Safe* (https://youtu.be/ oUxbggKtQN8).

Scan QR

9. Summarise the session by stressing that all forms of bullying (physical, social, verbal, and cyber) are wrong and that bullying will only stop if people speak out against bullying and lodge reports against the bullies.

Activity 2: Case Study (Daud's Story)

Learning Objectives

- To understand what cyber-bullying is and how it looks like.
- To know how to respond to and deal with cyber-bullying.
- To have better online behaviour towards others.

Time Required: 45 minutes

Materials

- A white board to record answers and responses.
- Some paper to write on.
- Projector to share the case study and questions or printed handouts – use the worksheet provided (Do not give the answers to the participants until they have provided theirs). Refer to the Discussion Points on pages 51-52.

Methodology

1. Inform the participants about the learning objectives.
2. Divide the participants into groups of 5-7 persons.
3. Start by sharing what is 'Cyber-bullying' (Refer to page 14).
4. Read the case study (Daud's Story) out loud and share a worksheet with each group.
5. Ask the participants to discuss and note down their answers.
6. Get the groups to respond to the questions (to save time, each group can answer one question and others can offer different opinions if any).

Case Study: Daud's Story

Daud is a 15-year-old boy who is active on social media. He is popular and has a number of friends both offline and online. One of his classmates, Sam, is jealous of the attention he is receiving. Sam creates a fake online account and starts to post negative messages and opinions about Daud. All of them are lies but some get re-circulated by others who do not know Daud very well. Daud tries to ignore these false postings as he does not know who is posting them. Occasionally he responds by saying they are all lies. This goes on intermittently for a few weeks until Sam posts a sexualised, edited image of Daud with the word 'homosexual' on it. This really stirs up things. Several people online and at school begin to call Daud a 'homo'. The more Daud denies this, the more the rumour spreads. Soon, more and more people gang up to tease him. Now a number of people send and share negative messages about him to his classmates. Daud is not able to sleep well and stops going to school.

Discussion Points

1. Has anyone been bullied offline or online before? Please share how you felt.

- Explore different responses from the participants.

2. Why do some people engage in cyber-bullying?

- There are many reasons why some people become cyber-bullies. Some do it to get revenge on others; some derive pleasure from seeing others suffer; some are bored or frustrated and use this as an outlet. Some cyber-bullies have been abused at home and take out their anger on others.
- Remember that people who are cyber-bullies may also need help from adults.

3. What can we do to prevent cyber-bullying? How can we behave better online?

- Treat others with the respect you would like to receive.
- Stop and think before you post or share your opinions, photos, videos of others online. If the post may harm or hurt someone, do not do it.
- Do not forward or share negative or embarrassing posts about anyone that are sent to you or that you see online.
- Never reveal your personal information or that of someone else online (i.e. address, phone number, school name or location).
- When you see cyber-bullying happening, stand up for the victim. The person who is being bullied needs our support and kindness.
- Tell a teacher, a trusted adult or your parents about any cyber-bullying you witnessed so as to get help.

4. **What should Daud do in his difficult situation?**

   - **STOP** – Stop responding to the online lies and bullies.
   - **TELL** – Talk to a person he trusts like parents or a trusted adult (teacher, doctor).
   - **DOCUMENT** – Take screenshots and record all the communications. **Do not** delete these communications as they are important to keep as evidence.
   - **REPORT and BLOCK** – Block the online account of the bully and get parents help to report the abuse to the relevant authorities (Refer to Appendix 3: Useful Contacts on pages 77-84).
   - **PASSWORDS** – Change all passwords on his application and online accounts immediately and make them stronger.
   - **THERAPY** – Get professional help from a counsellor to work through the trauma.

Worksheet: Cyber-bullying

Case Study: Daud's Story

Daud is a 15-year-old boy who is active on social media. He is popular and has a number of friends both offline and online. One of his classmates, Sam, is jealous of the attention he is receiving. Sam creates a fake online account and starts to post negative messages and opinions about Daud. All of them are lies but some get re-circulated by others who do not know Daud very well. Daud tries to ignore these false postings about him as he does not know who is posting them. Occasionally he responds by saying they are all lies. This goes on intermittently for a few weeks until Sam posts a sexualised, edited image of Daud with the word 'homosexual' on it. This really stirs up things. A number of people online and at school begin to call Daud a 'homo'. The more Daud denies this, the more the rumour spreads. Soon, more and more people gang up to tease him. Now a number of people send and share negative messages about him to his classmates. Daud is not able to sleep well and stops going to school.

Discussion

1. Has anyone been bullied offline or online before? Please share how you felt.

2. Why do some people engage in cyber-bullying?

3. What can we do to prevent cyber-bullying? How can we behave better online?

4. What should Daud do in his difficult situation?

Topic 5: Cyber-stalking and Cyber-harassment

Activity 1: Cyber-stalking

Learning Objectives

- To create an awareness and understanding on cyber-stalking.
- To get the participants to be careful while sharing their personal information online.

Time Required: 45 minutes

Materials

- WCC Cybersafety YouTube video *Cyber-stalking* and *Cyber Violence? Beware, Be Safe*.
- Laptop, sound speaker, projector, mahjong paper and marker pens.

Scan QR Scan QR

Methodology

1. Gather the participants together.
2. Ask them if they understand the term 'cyber-stalking'. If the participants say yes, get them to explain what their understanding is. If they say no, you have to explain to them what cyber stalking is.
   Cyber-stalking *is the repeated use of electronic communication to stalk a child with the intention to harass or threaten her/him.*
3. Tell the participants you are going to show them a video about cyber- stalking and after that there will be a discussion.
4. Play the WCC Cybersafety video *Cyber-stalking* (https://youtu.be/9jcDL9EnITA). At the end of the video, get them to express what they understand from the video. (Participants should be able to summarise what they saw). As the video is short, it might be necessary to play the video again.

Scan QR

5. Next ask them the following questions:
   a) What are the four main characteristics of cyber-stalkers?
   b) How does a person feel if she/he is being stalked online?
   c) Is stalking a person online a crime?
   d) What are some safety precautions to take?
   e) What can you do if someone stalks you online?

6. Once they have explored options on where they can seek help, play the WCC Cybersafety video *Cyber Violence? Beware, Be Safe* (https:// youtu.be/ oUxbggKtQN8).

7. Summarise the session by stressing the need to keep their online information private. Conclude that we need to be careful about the type of information we post online and who we approve as our friends/followers on social media.

Activity 2: Case Study (Li Jing's Story)

Learning Objectives

- To understand what cyber-stalking and cyber-harassment is and how it looks like.
- To know how to respond to and deal with cyber-stalking and cyber-harassment.

Time Required: 45 minutes

Materials

- A white board to record answers and responses.
- Some paper to write on.
- Projector to share the case study and questions or printed handouts – use the worksheet provided (Do not give the answers to the participants until they have provided theirs). Refer to the Discussion Points on pages 59-60.

Methodology

1. Inform the participants about the learning objectives.
2. Divide the participants into groups of 5-7 persons.
3. Start by sharing what cyber-stalking and cyber-harassment is (Refer to page 16).
4. Read the case study (story) out loud and share a worksheet with each group.
5. Ask the participants to discuss and note down their answers.
6. Get the groups to respond to the questions (to save time, each group can answer one question and others can offer different opinions if any).

Case Study: Li Jing's Story

Li Jing is a 16-year-old girl who had a boyfriend a year ago. The relationship did not turn out as she had hoped and she ended it. However, the boy was very keen to maintain the relationship. Li Jing had to be quite firm to tell him that it was over. She avoided meeting him and did not respond to any of his calls or messages.

Soon after she started receiving unusual messages on her Whatsapp from a number she did not know. Initially the person praised her for her beauty and capabilities and Li Jing did not mind this very much.

But as time went on the messages became more frequent, almost daily and took a more intimate tone. When she asked who it was, the response was a 'distant admirer'. She eventually blocked the person but found that similar messages were now coming from a different number. She became concerned as the person seemed to know so much about her. What finally frightened her was when an edited image of her in a sexual pose (using another person's body) was sent – the image suggested that her face was edited in just recently. Li Jing became very anxious, had difficulty sleeping and concentrating at school. She has become suspicious of all her friends.

Discussion Points

1. **Have you experienced stalking or harassment offline or online before? Please share how you felt.**
    - Explore different responses from the participants.

2. **How can we differentiate cyber-stalking or cyber-harassment from negative online comments?**
    - Anyone of us can receive negative online comments occasionally. If you have a high profile online account (many people follow you or you are well known), you may receive negative opinions more often.
    - The difference in cyber-stalking or cyber-harassment is that it is persistent, often from the same account and progressively getting worse. In addition, the person who is sending the unwanted messages seems to be aware of your personal life and relationships.

3. What should Li Jing do in this difficult situation?

- **STOP** – Stop responding to the online stalker.
- **TELL** – Talk to a person she trusts like parents or a trusted adult (teacher, doctor).
- **DOCUMENT** – Take screenshots and record all the communications. **Do not** delete these communications as they are important to keep as evidence.
- **REPORT and BLOCK** – Block the online account of the stalker (each time a new one appears) and get parents' help to report the abuse to the relevant authorities (Refer to Appendix 3: Useful Contacts on pages 77-84). A police report may be necessary.
- **PASSWORDS** – Change her passwords on all her application and online accounts immediately and make them stronger.
- **CHANGE** – Consider changing her hand phone number and email address. Reduce the amount of information available about her online.
- **THERAPY** – Get professional help from a counsellor to work through her trauma.

Worksheet: Cyber-stalking and Cyber-harassment

Case Study: Li Jing's Story

Li Jing is a 16-year-old girl who had a boyfriend a year ago. The relationship did not turn out as she had hoped and she ended it. However, the boy was very keen to maintain the relationship. Li Jing had to be quite firm to tell him that it was over. She avoided meeting him and did not respond to any of his calls or messages. Soon after she started receiving unusual messages on her Whatsapp from a number she did not know. Initially the person praised her for her beauty and capabilities and Li Jing did not mind this very much.

But as time went on the messages became more frequent, almost daily and took a more intimate tone. When she asked who it was, the response was 'a distant admirer'. She eventually blocked the person but found that similar messages were now coming from a different number. She became concerned as the person seemed to know so much about her. What finally frightened her was when an edited image of her in a sexual pose (using another person's body) was sent – the image suggested that her face was edited in just recently. Li Jing became very anxious, had difficulty sleeping and concentrating at school. She has become suspicious of all her friends.

Discussion

1. Have you experienced stalking or harassment offline or online before? Please share how you felt.

2. How can we differentiate cyber-stalking or cyber-harassment from negative online comments?

3. What should Li Jing do in this difficult situation?

Topic 6: Pornography

Activity: Case Study (Jason's Story)

Learning Objectives

- To understand what child sexual abuse material is and its impact on children.
- To know how to respond to and deal with inappropriate sexual content.

Time Required: 45 minutes

Materials

- A white board to record answers and responses.
- Some paper to write on.
- Projector to share the case study and questions or printed handouts– use the worksheet provided (Do not give the answers to the students until they have provided theirs). Refer to the Discussion Points on page 60.

Methodology

1. Inform the participants about the learning objectives.
2. Divide the participants into groups of 5-7 persons.
3. Start by sharing what is 'Pornography' (Refer to page 18).
4. Read the case study (Jason's Story) out loud and share a worksheet with each group.
5. Ask the participants to discuss and note down their answers.
6. Get the groups to respond to the questions (to save time, each group can answer one question and others can offer different opinions if any).

Case Study: Jason's Story

Jason is a 14-year-old boy who is keen to be part of the 'gang' – a group of his male peers and slightly older boys who hang out together both offline (at the mall) and online in a closed Telegram group. He is told that to join them, as an initiation, he must share five porn images or two videos of women having sex on the first day of joining the Telegram group. Jason is very keen to join them, so he downloads images to share and is invited into the group. Now everyday Jason sees porn images or videos shared in the group. Initially it was stimulating and he started masturbating more often but overtime he felt degraded and sullied. However, he wants to remain part of the group and also wants to continue seeing porn images.

Discussion Points

1. **Has anyone ever sent you images of naked persons before? Have you accidentally seen naked images or videos of people online? Please share how you felt.**
    - Explore different responses from the participants.

2. **What will happen to someone who frequently watches pornography?**
    - Discuss the negative effects of pornography on children.
    - Also speak about how pornography degrades our perspective of women and girls in general.

3. **How do we respond when we receive sexually explicit materials, and how do we minimise exposure to these materials?**
    - When you are curious and have questions about sex and your body, ask an adult you trust like your parents, teacher or doctor, rather than look it up online.
    - Ask your parents how you can configure your mobile device or computer to do safe online searches.
    - Ask your parents to see how adverts can be blocked on your mobile.
    - If you accidently see pornography online, immediately close that page.
    - Tell a teacher, a trusted adult or your parents if anyone sends you pornographic material.

    Always remember to treat others with the respect you would like to receive, and this includes online images.

4. **What should Jason do in his situation?**
    - **STOP** – Stop looking at the pornographic images on his Telegram account.
    - **TELL** – Talk to a person he trusts like parents or a trusted adult (teacher, doctor).
    - **LEAVE** – Take the strong decision to leave/exit the group.
    - **FIND** – Find new friends that are more wholesome.
    - **THERAPY** – Get professional help from a counsellor to work through the sexualisation that has occurred.

Worksheet: Pornography

Case Study: Jason's Story

Jason is a 14-year-old boy who is keen to be part of the 'gang' – a group of his male peers and slightly older boys who hang out together both offline (at the mall) and online in a closed Telegram group. He is told that to join them, as an initiation, he must share five porn images or two videos of women having sex on the first day of joining the Telegram group. Jason is very keen to join them, so he downloads images to share and is invited into the group. Now everyday Jason sees porn images or videos shared in the group. Initially it was stimulating and he started masturbating more often but over time he felt degraded and sullied. However, he wants to remain part of the group and also wants to continue seeing porn images.

Discussion

1. Has anyone ever sent you images of naked persons before? Have you accidentally seen naked pictures or videos of people online?
   Please share how you felt.

2. What will happen to someone who frequently watches pornography?

3. How do we respond when we receive sexually explicit materials, and how do we minimise exposure to these materials?

4. What should Jason do in his situation?

Topic 7: Generative Artificial Intelligence

Activity: Case Study (Sarah's Story)

Learning Objectives

- To understand what sexually explicit deepfakes are and their impact on us.
- To know how to respond when someone creates sexually explicit deepfakes of a child.

Time Required: 45 minutes

Materials

- A white board to record answers and responses.
- Some paper to write on.
- Projector to share the case study and questions or printed handouts – use the worksheet provided (Do not give the answers to the students until they have provided theirs). Refer to the Discussion Points on pages 63-64.

Methodology

1. Inform the participants about the learning objectives.
2. Divide the participants into groups of 5-7 persons.
3. Start by sharing what sexually explicit deepfakes are (Refer to page 20).
4. Read the case study (Sarah's Story) out loud and share a worksheet with each group.
5. Ask the participants to discuss and note down their answers.
6. Get the groups to respond to the questions (to save time, each group can answer one question and others can offer different opinions if any).

Case Study: Sarah's Story

Sarah is a 15-year-old girl who is active on social media, especially Tik Tok and Instagram. She often posts her favourite images taken of her family and herself on social media – lovely snapshots of happy memories.

One day a message came from a close friend. She asked Sarah if she had seen images of herself posted on a social media site by an anonymous individual. Sarah clicked the link that was shared with her to check it out. She was suddenly not able to breathe and felt cold all over – there were a number of naked images of her posted online – it was her face but not her body. The images looked so real, so 'undeniably' her, but she knew it wasn't. She recognised that some of the deepfakes had been made using images from a recent beach trip that are posted online. Panic seized her, her heart pounded and her hands trembled. She felt her world turn upside-down as she stared at the horrifying images – thinking of all her school friends and others that might have seen them.

Over the next few days, she couldn't eat or sleep. Every notification on her phone made her jump. She felt intense shame even though she had done nothing wrong. She was so afraid her family might see them. She stopped going to school and made some excuses to her parents about being unwell. Sarah felt trapped, ashamed, and utterly alone in a nightmare she didn't understand. The deepfakes had not just altered her image; it had stolen her peace, her trust, and her sense of safety in the world.

Discussion Points

1. **Has anyone seen or used AI-generated or edited images? Please share your experience.**
    - Explore different responses from the participants.

2. **Is it OK to generate deepfake nudes of another person — even though the content isn't real?**
    - Explain every person's right to privacy, bodily autonomy, and sexual integrity. Note that deepfake nudes are often created by a peer. Note that this is a criminal activity and that action can be taken against the person who created or posted the deepfakes under Malaysian laws. Also mention that we should not create AI-generated materials of another person without their explicit approval.

3. **How do you think sexualised deepfakes impacts the person whose images has been used? How would you feel if some posted naked deepfake images of you?**

    - Sexualised deepfakes impacts the victim deeply. They feel violated, have a loss of dignity, feel isolated (do not know who to trust) and feel insecure (unsafe). It damages their relationships in society and they fear they will be blamed for what has happened. Most have serious anxiety and depression and some resort to self-harm.

4. **How should Sarah deal with the deepfake nude images?**

    - **STOP** – Do not respond to the deepfake online posts.
    - **TELL** – Talk to a person she trusts like parents or a trusted adult (teacher, doctor).
    - **DOCUMENT** – Take screenshots and record all the communications – even though this is painful and a reminder of the abuse. They are important to keep as evidence.
    - **REPORT** – Get parents' help to report the abuse to the relevant authorities (Refer to Appendix 3: Useful Contacts on pages 77-84). A police report is necessary.
    - **CHANGE** – Consider changing her online posting behaviour (less images of herself) and restrict access to more private postings.
    - **THERAPY** – Get professional help from a counsellor to work through her trauma.

5. **How can family, friends and classmates support her?**

    - We need to provide support for Sarah and her family. Remind her that it is not her fault. Encourage her to come to school and continue to maintain our relationship with her. The authorities should keep Sarah and her family updated about actions being taken.

Worksheet: Generative Artificial Intelligence

Case Study: Sarah's Story

Sarah is a 15-year-old girl who is active on social media, especially Tik Tok and Instagram. She often posts her favourite images taken of her family and herself on social media – lovely snapshots of happy memories.

One day a message came from a close friend. She asked Sarah if she had seen images of herself posted on a social media site by an anonymous individual. Sarah clicked the link that was shared with her to check it out. She was suddenly not able to breathe and felt cold all over – there were a number of naked images of her posted online – it was her face but not her body. The images looked so real, so 'undeniably' her, but she knew it wasn't. She recognised that some of the deepfakes had been made using images from a recent beach trip that are posted online. Panic seized her, her heart pounded and her hands trembled. She felt her world turn upside-down as she stared at the horrifying images – thinking of all her school friends and others that might have seen them.

Over the next few days, she couldn't eat or sleep. Every notification on her phone made her jump. She felt intense shame even though she had done nothing wrong. She was so afraid her family might see them. She stopped going to school and made some excuses to her parents about being unwell. Sarah felt trapped, ashamed, and utterly alone in a nightmare she didn't understand. The deepfakes had not just altered her image; it had stolen her peace, her trust, and her sense of safety in the world.

Discussion

1. Has anyone seen or used AI generated or edited images? Please share your experience.

_____

_____

_____

2. Is it OK to generate deepfake nudes of another person — even though the content isn't real?

_____

_____

_____

3. How do you think sexualised deepfakes impacts the person whose images has been used? How would you feel if some posted naked deepfake images of you?

4. How should Sarah deal with the deepfake nude images?

5. How can family, friends and classmates support her?

Appendix 1: Red Flags – Tips for Children to Stay Safe Online

How can you know the person (stranger) you meet online is a safe person? Always trust your own intuition and your inner voice. If you feel uncomfortable, you should speak to a trusted adult.

Below are red flags (warning signs ⚠) that suggest this is an unsafe online interaction when the online person:

- ⚠ Praises you a lot, especially your appearance ("you look so pretty or handsome").
- ⚠ Tries to move the relationship/communication to a private one (one-to-one).
- ⚠ Asks you to keep the relationship secret.
- ⚠ Inquisitive about your personal life and asks for information (e.g. address, hand phone number, etc.).
- ⚠ Wants to send you gifts.
- ⚠ Asks you for an intimate photograph (i.e. a photograph that shows part of your body naked or private parts).
- ⚠ Wants to meet face-to-face.

What to Do When Things Go Wrong?

Below are immediate steps and actions you can take:

- **STOP** – Stop the communication with the offender or bully and do not give in to any more demands.
- **TELL** – Talk to a person you trust like parents or a trusted adult (teacher, doctor).
- **DOCUMENT** – Take screenshots and record all the communications. **Do not** delete these communications as they are important to keep as evidence.
- **BLOCK** – Block the phone number and online account of the offender. At times you may need to get a new phone number and email address.
- **REPORT** – Get parents' or a trusted adult's help to report the abuse to the relevant authorities like the police or Social Welfare Department and the online account to its platforms.
- **PASSWORDS** – Change all your application and online accounts' passwords immediately and make them stronger.
- **THERAPY** – Get professional help from a counsellor to work through your trauma and help you cope with your feelings.

Appendix 2: Laws Related to Cyber Violence and Child Sexual Crimes

The aim of the laws is to punish and rehabilitate the offenders so that they will not commit the offences again. When the victim makes a police report, it is to help her/him to seek justice for the crime committed. Even though the victim may not get any monetary compensation from the prosecution, it should stop further abuse of the victim and prevent the perpetrator from abusing other children.

Penal Code

SECTION	OFFENCE	PUNISHMENT
292	When a person sells, distributes, produces, possesses, etc., any forms of obscene materials.	Imprisonment for a maximum of 3 years or fine or both.
293	When a person sells, distributes, circulates, etc., any forms of obscene materials to any person under the age of 20.	Imprisonment for a maximum of 5 years or fine or both.
377CA	Sexual connection by the introduction of any object into the vagina or anus of another person without consent.	Imprisonment for a minimum 5 years, maximum of 30 years and whipping.
377D	Outrages on decency.	Imprisonment for a maximum of 2 years.
503, 506 & 507	When a person threatens another with any injury to his person, reputation or property with the intent to cause alarm to that person, even by using an anonymous communication.	Imprisonment for maximum 2 years or fine or both. In addition, imprisonment maximum 2 years for using anonymous communication.
507A	Stalking. This may include communicating or attempting to communicate with a person in any manner or by any means.	Imprisonment for a maximum of 3 years or with fine or both.
507B	Causing harassment, distress, fear, or alarm.	Imprisonment for a maximum of 3 years or with fine or both.

507C	Causing harassment, distress, fear, or alarm to a person likely to feel harassed, distressed, fear or alarmed.	Imprisonment for a maximum of 1 year or fine or both.
507D(1)	Causing a person to believe that harm will be caused.	Imprisonment for a maximum of 1 year or with fine or both.
507D(2)	Causing a person to believe that harm will be caused, and if the person provoked attempts to commit suicide or commits suicide as a result of provocation.	Imprisonment for a maximum of 10 years or fine or both.
507E	Publishing, circulating or making available any identity information to cause harassment, distress, fear or alarm.	Imprisonment for a maximum of 3 years or fine or both.
507F	Publishing, circulating or making available any identity information to cause a person to believe that harm will be caused; or does so in a way that is likely to facilitate harm to a person or his related person.	Imprisonment for a maximum of 1 year or fine or both.
507G	Definitions of "harm", "identity information" and "related person" (in relation to Sections 507D, 507E and 507F). Harm means harm to a person's body, mind, reputation or property, including psychological harm. Identity information means any information that identifies or purports to identify a person. Related person means, in relation to a person, any person whose safety or well-being would reasonably be expected to be of concern of the first-mentioned person.	See Sections 507D, 507E and 507F.
509	Word or gesture intended to insult the modesty of any person.	Imprisonment for a maximum of 5 years or fine or both.

Child Act 2001

SECTION	OFFENCE	PUNISHMENT
15	Restrictions on media reporting and publication – Any mass media shall not reveal the name, address or educational institution, picture or include any particulars calculated to lead to the identification of any child involved in any criminal court proceedings including investigation stage under this Act.	Liable to an imprisonment for a maximum of 5 years or maximum RM10,000 fine or both.
27, 28, 29	Duty to inform – A medical officer or medical practitioner, or member of the family, or childcare provider who believes that a child is physically or emotionally injured due to being ill-treated, neglected, abandoned or exposed or is sexually abused, shall immediately inform a Social Welfare Officer.	Failure to inform – Liable to imprisonment for a maximum of 2 years or maximum RM5,000 fine or both.
29A	Duty to inform – Any person other than those referred in Sections 27,28,29 who believes that a child is physically or emotionally injured due to being ill-treated, neglected, abandoned or exposed or is sexually abused, may inform a Social Welfare Officer.	No penalty.
31(1)	Ill-treatment of children. Any person who having the care of a child – a) abuses, neglects, abandons or exposes the child or acts negligently in a manner likely to cause him physical or emotional injury; or b) sexually abuses the child or causes or permits him to be so abused.	Liable to a maximum RM50,000 fine or imprisonment for a maximum of 20 years or both. In addition, may be ordered to execute a bond for good behaviour and perform community service.

32	Children not to be used for begging or any illegal activities – Any person who causes a child to carry out any such activities will be punished.	Liable to a maximum RM20,000 fine or imprisonment for a maximum of 5 years or both. In addition, may be ordered to execute a bond for good behaviour and perform community service.
116	Any person who gives any information that a child is in need of protection shall not incur any liability for defamation or otherwise, shall not be held to constitute a breach of professional etiquette or ethics or a departure from accepted standards of professional conduct for giving such information.	No penalty.

Sexual Offences Against Children Act 2017

The Act provides for sexual offences against children which are not adequately covered by the Penal Code and Child Act.

Among the offences addressed under this Act are those involving child sexual abuse material, child grooming, physical and non-physical sexual assaults against children, and, punishment for these offences has been enhanced.

SECTION	OFFENCE	PUNISHMENT
5	Making, producing, directing the making or production of child sexual abuse material.	Imprisonment for a maximum of 30 years and minimum of 6 strokes of whipping.
6	Making, preparation to make, produce or direct the making or production of child sexual abuse material.	Imprisonment for a maximum of 10 years and liable for whipping.
7	Using a child in making, producing, directing the making or production of child sexual abuse material.	Imprisonment for a maximum of 20 years and minimum 5 strokes of whipping.
8	Exchanging, publishing of child sexual abuse material.	Imprisonment for a maximum of 15 years and minimum 3 strokes of whipping.
9	Selling child sexual abuse material to a child.	Imprisonment maximum 15 years and minimum 5 strokes of whipping.
10	Accessing child sexual abuse material.	Liable to imprisonment maximum 5 years or fine maximum RM10,000 or to both.
11	Sexually communicating with a child (except for education, scientific/ medical purposes).	Imprisonment maximum 3 years.
12	Child grooming.	Imprisonment maximum 5 years and liable for whipping.
13	Meeting following child grooming.	Imprisonment maximum 10 years and liable for whipping.
14	Physical sexual assault on a child.	Imprisonment maximum 20 years and liable for whipping.

15	Non-physical sexual assault on child e.g. makes a child exhibits the child's body to be seen by others for sexual purposes.	Imprisonment maximum 10 years or fine maximum RM20,000 or both.
15A	Sexual performance by a child.	Imprisonment maximum 20 years and liable for a fine maximum RM50,000.
15B	Sexual extortion of a child.	Imprisonment maximum 10 years.
16	If a person in a relationship of trust commits any offence under this Act, punishment to be more severe. Persons in relationship of trust include: a) parent/guardian/relative b) babysitter c) teacher/lecturer/warden d) healthcare providers e) coach f) public servant	In addition to punishment for such an offence, will be punished with further imprisonment maximum 5 years and whipping minimum 2 strokes.
19	Failure to give information – Any person who fails to give information of any child sexual abuse case to the police commits an offence.	Liable to a fine maximum RM5,000.
25	Provisions regarding whipping: If a person convicted under this Act is a male over 50 years of age.	Is still liable for whipping.
26	Rehabilitative counselling.	The court may, in addition to any punishment imposed, order a period of rehabilitative counselling on the person convicted within the period of his detention.
27	Police supervision.	When a person is convicted of any offence under this Act, the court shall direct that he be subject to the supervision of the police for a period of not less than one year and not more than three years after the expiration of the sentence passed on him.

Communications and Multimedia Act 1998

SECTION	OFFENCE	PUNISHMENT
211	Indecent, obscene, false, menacing, or grossly offensive content (by content applications service provider).	Imprisonment for a maximum of 10 years or maximum RM1 million fine or both and also liable to a further fine of RM100,000 for every day or part of a day during which the offence is continued after conviction.
233	Improper use of network facilities or network service to communicate content which is obscene, indecent, false, menacing or grossly offensive with intent to annoy, abuse, threaten, harass or commit an offence involving fraud or dishonesty against, any person.	Imprisonment for a maximum of 2 years or maximum RM500,000 fine or both and also liable to a further fine of RM5,000 for every day during which the offence is continued after conviction. Where the offence has been committed against a child below 18 years old, the convicted offender is liable to imprisonment for a maximum of 5 years or maximum RM500,000 fine or to both and also liable to a further fine of RM5,000 for every day or part of a day during which the offence is continued after conviction. Where obscene communication is provided for commercial purposes, the convicted offender is liable to imprisonment for a maximum of 5 years or maximum RM1 million fine or to both and also liable to a further fine of RM10,000 for every day or part of a day during which the offence is continued after conviction.

Online Safety Act 2025

The Online Safety Act 2025 aims to promote and enhance online safety in Malaysia by regulating harmful content and providing for duties and obligations on applications service providers, content applications service providers and network service providers.

The Act defines the following as harmful content:

1. Content on child sexual abuse material as provided for under section 4 of the Sexual Offences Against Children Act 2017.
2. Content on financial fraud.
3. Obscene content including content that may give rise to a feeling of disgust due to lewd portrayal which may offend a person's manner on decency and modesty.
4. Indecent content including content which is profane in nature, improper and against generally accepted behaviour or culture.
5. Content that may cause harassment, distress, fear or alarm by way of threatening, abusive or insulting words or communication or act.
6. Content that may incite violence or terrorism.
7. Content that may induce a child to cause harm to himself.
8. Content that may promote feelings of ill-will or hostility amongst the public at large or may disturb public tranquility
9. Content that promotes the use or sale of dangerous drugs.

Of these, content on child sexual abuse material and financial fraud are defined as priority harmful content.

**Note: From 1 June 2026, it is mandatory for social media platforms to verify the age of users. Children under 16 are not allowed to register. This initiative is to protect children from online exploitation.*

The Act also imposes several duties on applications service providers (ASPs) and content applications service providers (CASPs), which includes:

SECTION	DUTIES OF ASPs AND CASPs
13	Duty to implement measures to mitigate risk of exposure to harmful content
14	Duty to issue guidelines to user
15	Duty to enable user to manage online safety
16	Duty to make available mechanism for reporting harmful content
17	Duty to make available mechanism for user assistance
18	Duty to protect online safety of child user
19	Duty to establish mechanism for making priority harmful content inaccessible
20	Duty to prepare Online Safety Plan

Non-compliance to duties can lead to financial penalty up to RM10 million.

This Act also outlines reporting mechanisms of harmful content.

SECTION	REPORTING MECHANISMS
21	Report to licensed applications service provider and licensed content applications service provider
22	Report to licensed applications service provider and licensed content applications service provider on priority harmful content
23	Report to licensed applications service provider and licensed content applications service provider on harmful content
24	Report to Malaysian Communications and Multimedia Commission
25	Report to Malaysian Communications and Multimedia Commission on harmful content

Under the Act, an Online Safety Committee is established to advise and give recommendations to the Malaysian Communications and Multimedia Commission (MCMC) on matters related to online safety.

The Act also provides for the establishment of an Online Safety Appeal Tribunal to review decisions made by the MCMC under the Act.

Appendix 3: Useful Contacts

Below is a list of useful contacts in Malaysia to support children in child protection, provide counselling, and other helpful resources. Note that not all can provide on-site support or liaison with governmental agencies; some only offer advice and counselling. Most of the services listed here offer free services. Kindly check with the individual organisations or their websites for the services offered.

GOVERNMENT AGENCIES

Talian Kasih
Hotline: 15999
WhatsApp: 019-261 5999
Mobile app: Talian Kasih app

Malaysian Communications & Multimedia Commission
Hotline (office hours only): 1800-188-030
E-mail: aduanskmm@mcmc.gov.my
Online Complaint: https://aduan.skmm.gov.my

Bullying Complaint Portal by Ministry of Education
Office number: 03-8884 9325
Telephone and WhatsApp: 014-800 9325
SISPAA (Online Complaint): https://moe.spab.gov.my/eApps/system/index.do
Website: https://aduanbuli.moe.gov.my/
Note: This complaint channel only accepts complaints related to bullying that occurs among students in schools under the Ministry of Education only.

NON-GOVERNMENT ORGANISATIONS (NGOs)

Women's Centre for Change (WCC)
241 Jalan Burma, 10350 Penang.
Tel: 04- 228 0342 / 011-3108 4001
E-mail: wcc@wccpenang.org
Website: wccpenang.org

Pusat Perkhidmatan Wanita (PPW)
13 Lorong Sutera 6, Taman Sutera, 13700 Seberang Jaya, Penang.
Tel: 04-398 8340 / 016-439 0698
E-mail: ppw@wccpenang.org

All Women's Action Society (AWAM)
85, Jalan 21/1, Sea Park, 46300 Petaling Jaya, Selangor.
Tel: 03-7877 4221
Telenita Helpline: 016-237 4221 / 016-228 4221
E-mail: awam@awam.org.my
Website: awam.org.my

Advocates for Non-discrimination and Access to Knowledge (ANAK)
Beverly Hills Plaza, Jalan Bundusan, 88300 Kota Kinabalu, Sabah.
Tel/WhatsApp: 014-670 0309
E-mail: hello@anaksabah.org
Website: www.anaksabah.org

Bar Council Child Rights Committee
E-mail: pad@malaysianbar.org.my
Website: www.malaysianbar.org.my

Bar Council Legal Aid Centre
Selangor Tel: 03-5510 7007
KL Tel: 03-2691 1121 / 03-2692 1122
Penang Tel: 04-261 7451
Website: www.malaysianbar.org.my

Befrienders Kuala Lumpur
E-mail: sam@@befrienders.org.my
Website: www.befrienders.org.my

Befrienders Penang
Blok 104 – 1A, Mewah Court, Jalan Tan Sri Teh Ewe Lim, 11600 Penang.
Tel: 04-291 0100
WhatsApp: 011-5670 6261
E-mail: pat@befpen.org
Website: www.befpen.org

Befrienders Kota Kinabalu
Tel: 088-335 793
E-mail: befrienderskk@gmail.com

Befrienders Kuching
P.O Box 19, Pejabat Pos Besar, Jalan Tun Abang Haji Openg,
93670 Kuching, Sarawak.
Tel: 082-242 800
E-mail: sam@befrienderskch.org.my

Bodhi Counselling, Kuching Buddhist Society
Lot 1912, Q130A, Iris Grden, 93200 Kuching, Sarawak.
Tel: 082-256 428 / 082-256 429 / 011-6330 5990 (by appointment only)
E-mail: putifudao@gmail.com
Website: http://counselling.kbs.org.my

Buddhist Gem Fellowship (Gem Helpline)
Provides free counselling and emotional support
D-G-2, Block D, Taipan 1, Jalan PJU 1A/3K, Ara Damansara,
47500 Petaling Jaya, Selangor.
Gem Helpline: 011-2528 9610 / 011-5994 4384
Instagram: @gem.helpline

Buddy Bear (Human Kind)
Provides emotional and psycho-social support to children (6 to 18 years old)
Helpline: 1-800-18-2327
Instagram: @buddybear.humankind

Calvary Life Ministries
4, Jalan Damansara Endah, Damansara Heights, 50490 Kuala Lumpur.
Tel: 03-2095 6360
E-mail: clm@clm.org.my
Website: https://www.clm.org.my/counselling.html

Childline Foundation
2, Jalan SS3/52, Sungai Way Subang, 47300 Petaling Jaya, Selangor.
Tel: 016-333 4228
Website: www.childlinefoundation.com

CRIB (Child Rights Innovation & Betterment) Foundation
Tel: 012-385 5451 / 012-607 5990
E-mail: crib.foundationmy@gmail.com
Facebook: CRIB Foundation

Eden Community Service Center
11-1, Jalan Bakar Sampah, 86000 Kluang, Johor.
Tel: 018-376 0601
Website: http://eden.org.my/

Emmaus Centre of Counselling, Church of St Francies Xavier
Tel: 03-7957 7136
WhatsApp: 014-669 1516
E-mail: emmauscounselor.sfx@gmail.com
Website: http://sfx.com.my/

Family Empowerment Society (FAME)
E-mail: familyempowerment.info@gmail.com
Instagram: @fame.malaysia

Global Shepherds Headquarters
Tel: 03-4265 1749
E-mail: info@globalshepherds.my
Website: globalshepherds.my

Global Shepherds Keningau
Lot 188, Lorong 2G, Taman Jutaya 2, Jalan Apin-Apin, 89000 Keningau, Sabah.
Hotline: 019-260 6397

Global Shepherds Kota Kinabalu
No. 529, Off Jalan Tuaran Road, Likas, 88000 Kota Kinabalu, Sabah.

Global Shepherds Sandakan
Rumah Orchid CL75095055, Jalan Cecily, 90000 Sandakan, Sabah.
Hotline: 012-321 1698

Good Shepherd
KL HQ: c/o Villamaria Good Shepherd, Lorong Setiabistari 2, Medan Damansara, 50490 Kuala Lumpur.
Tel: 012-775 3020
E-mail: info@goodshepherd.my
Website: goodshepherd.my/EN/home

Good Shepherd Ipoh
34, Jalan Wayang, Taman Pertama, 30100 Ipoh, Perak.
Tel: 05-242 0388

Good Shepherd Sabah
Walai Good Shepard
529, Mile 3.5, Jalan Tuaran, 88450 Kota Kinabalu, Sabah.
Tel: 088-652 410

Youth-PREP Centre
Lot.25, First Floor, Block E Phase, 2, Alamesra, 88400 Kota Kinabalu, Sabah.
Tel: 014-866 0224

Internet Watch Foundation (IWF) Malaysia
Reporting Portal: https://report.iwf.org.uk/my_en/

Johor Women's League (JEWEL)
Tel: 011-6118 8913 / 016- 253 5226
E-mail: info.jewelmalaysia@gmail.com
Website: jewelmalaysia.org

Justice for Sisters
E-mail: info@justiceforsisters.org
Website: https://justiceforsisters.org/en/

KawanBAH Careline
Tel: 012-775 3020
WhatsApp: 012-775 3020

KRYSS Network
107A-A, Block A, Ground Floor, Jalan SS2/72, 47300 Petaling Jaya, Selangor.
Instagram: @kryssnetwork

Life Line Association Malaysia
No. 1-3, 3rd Floor, Jalan Jelatek 1, Pusat Perniagaan Jelatek, Setiawangsa, 54200 Kuala Lumpur.
Tel: 03-4266 6195 (Admin)
Counseling Hotline: 15995
E-mail: counselling@lifeline.org.my
Website: lifeline.org.my

Malaysian Mental Health Association
8, Jalan 4/33, Off Jalan Othman, 46050 Petaling Jaya, Selangor.
Tel: 03-2780 6803/ 017-613 3039
E-mail: admin@mmha.org.my
Website: www.mmha.org.my

Malaysians Against Pornography
E-mail: malaysiansagainstpornography@gmail.com
Website: http://malaysiansagainstpornography.com/

Mental Health Association of Sarawak
Tel: 016-976 4623
E-mail: counselling@mhasarawak.com
Website: mhasarawak.com

New Era College Counselling Centre
Block C, Lot 5, Seksyen 10, Jalan Bukit, 43000 Kajang, Selangor.
Tel: 03-8740 6392 / 03-8210 3709
E-mail: counselling@newera.edu.my
Website: www.newera.edu.my/counselling_centre/index_e.php

Perak Women for Women (PWW)
15, Market Street, 30000 Ipoh, Perak.
E-mail: perakwomenforwomen@gmail.com
Facebook: Perak Women for Women

Protect and Save the Children (P.S. The Children)
Suite E-10-21, Level 10, Menara Melawangi, Amcorp Mall, Amcorp Trade Centre,
No. 18 Jalan Persiaran Bart, 46050 Petaling Jaya, Selangor.
WhatsApp: 018-236 3252
E-mail: protect@psthechildren.org.my
Website: psthechildren.org.my

Purple Lily
Changlin Park, Jalan Tabuan, 93100 Kuching.
Tel: 082-295 180 / 082-231 803
WhatsApp: 019-874 1251
E-mail: purplelily.kuching@gmail.com
Website: purplelily.org

Rahmah Support Team
No. 1, Jalan Bukit Bintang, Bukit Bintang, 55100 Kuala Lumpur.
Tel: 018-354 2293
E-mail: rahmah.centre24@gmail.com
Facebook: Rahmah Support Team -RST

Sarawak Women for Women Society (SWWS)
Unit 16, Level 4, La Promenade Mall 2, Hock Seng Lee Tower,
Kuching-Samarahan Expressway, 94300 Kota Samarahan, Sarawak.
Tel: 082-368 853 / 013-804 4285
SWWS Crisis Phoneline: 016-582 2660
E-mail: info@sarswws.org
Website: sarswws.org

Shelter Home for Children
No 2, Lorong Timur, 46000 Petaling Jaya, Selangor.
Tel: 03-7955 0663
WhatsApp: 011-2611 0663
E-mail: office@shelterhome.org
Website: www.shelterhome.org

SIS Forum (Malaysia)
No. 4 Lorong 11/8E, 46200 Petaling Jaya, Selangor.
Tel: 03-7960 3357 / 5121 / 6733
E-mail: sis@sistersinislam.org.my
Website: sistersinislam.org

Sneham Malaysia Welfare Association
Has a Tamil focus (also BM & English)
Tel: 1-800-22-5757 (toll free)
E-mail: snehammalaysia@gmail.com
Facebook: Pertubuhan Kebajikan Sneham Malaysia

SUKA Society
PO Box 013 Jalan Sultan, 46700 Petaling Jaya, Selangor.
Tel: 03-7877 4227
E-mail: enquiry@sukasociety
Website: www.sukasociety.org

Tenaganita
12, Jalan 6/11, Seksyen 6, 46000 Petaling Jaya, Selangor.
Tel: 03-7770 3671 / 3691
Hotline: 012-335 0512 / 012-339 5350 (24hrs for emergencies)
E-mail: general@tenaganita.net
Website: tenaganita.net

Thrive Well
Unit L5-11, Wisma BU8, No. 11, Lebuh Bandar Utama, 47800 Petaling Jaya, Selangor.
Tel: 018-900 3247
E-mail: info@thethrive.center
Website: https://www.thethrive.center/

Than Hsiang Mitra Welfare Center – KL (Mitraline)
196, Batu 3 1/4, Jalan Klang Lama, 58000 Kuala Lumpur.
Tel: 03-7971 9876
WhatsApp: 011-3601 8303
Hotline: 03-7981 5300 / 03-7981 5301
E-mail: mitraklcounselling@gmail.com
Website: https://kl.thanhsiang.org/mitra-welfare-center/mitraline/

Than Hsiang Mitra Welfare Center Penang (Mitraline)
132, Jalan Sultan Azlan Shah, 11900 Bayan lepas 11900 Bayan Lepas, Penang.
Tel: 04-313 1141 (counselling appointment and welfare assistance)
Hotline: 04-642 9429
Facebook: Than Hsiang Mitra Welfare Center Penang

The Bridge Communication
40, Lorong 6E/91, Taman Shamelin Perkasa, Batu 3 1/2, Jalan Cheras,
56100 Kuala Lumpur.
Tel: 03-9286 4046
WhatsApp: 017-901 6782
E-mail: b_counsel@yahoo.com
Website: https://bridge.org.my/

Voice of the Children
Facebook: Voice of the Children

Women's Aid Organisation (WAO)
P.O.Box 493, Jalan Sultan 46760 Petaling Jaya, Selangor.
Tel: 03-7957 5636
Hotline: 03-3000 8858
SMS/WhatsApp TINA: 018-988 8058 (24hrs)
Email: info@wao.org.my
Website: wao.org.my

Yayasan Chow Kit
No. 19, Jalan Belia, Off Jalan Tunku Abdul Rahman, 50350 Kuala Lumpur.
Tel: 03-2602 0892
Email: admin@yck.org.my
Website: https://yck.org.my/

Young Buddhist Association of Malaysia (YBAM) PELITA Psychological Unit
9, Jalan SS25/24, Taman Mayang, 47301 Petaling Jaya, Selangor.
Hotline: 03-2022 5505
E-mail: pelita@ybam.org.my
Website: http://www.ybam.org.my

Women's Centre for Change

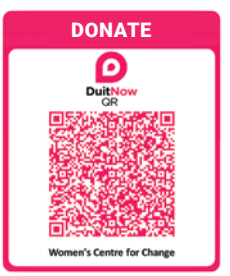
PPM-012-07-07011985

Women's Centre for Change, Penang (WCC) is a non-profit, registered organisation dedicated to the elimination of violence against women and children, and the promotion of gender equality and social justice.

Established in 1985, we provide services in counselling and court support, and referrals to temporary shelter. WCC also conducts outreach programmes in schools and communities, and advocates for legal and policy reforms affecting women and children.

PPW PUSAT PERKHIDMATAN WANITA

Pusat Perkhidmatan Wanita (PPW) is a smart partnership set up in 2009 between WCC and the Penang State Government where the state allocates an annual grant for WCC to manage PPW operations in Seberang Perai.



WCC is a tax-exempt organisation and is totally dependent on donations and sponsorship to support our work. We welcome donations.

Pusat Kesedaran Wanita
CIMB 860 1023057

**Any donation of RM50 and above will be issued a tax exempt receipt.*

WCC
Women's Centre for Change

241, Jalan Burma, 10350 Penang, Malaysia.
+604-228 0342 +6011-3108 4001
wcc@wccpenang.org

www.wccpenang.org

PPW PUSAT PERKHIDMATAN WANITA

13, Lorong Sutera 6, Taman Sutera,
13700 Seberang Jaya, Penang, Malaysia.
+604-398 8340 +6016-439 0698
ppw@wccpenang.org

WCC Penang

ISBN 978-967-16908-9-5