Online Child Safety: The Myth and Reality of Cybersecurity Laws in Malaysia

***Mazlina Mohamad Mangsor., Mazlifah Mansoor., Noraiza Abdul Rahman**

Faculty of Law, Universiti Teknologi MARA Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.91100351

Received: 26 November 2025; Accepted: 03 December 2025; Published: 11 December 2025

ABSTRACT

The accelerated growth of online engineering has amplified both possibilities and risks for children in a digital environment. In 2024-2025, Malaysia has inaugurated legal transformations with the enactment of Cyber Security Act 2024 and Online Safety Act 2025; and the amendment of Communications and Multimedia (Amendment) Act 2025, Penal Code (Amendment) 2025, and Personal Data Protection (Amendment) Act 2024. The main purpose is to enhance protections facing harmful content and digital exploitation. This paper aims to examine the extent of the online safeguards for child safety under the newly introduced digital legislation in Malaysia and to compare them to those of the Australian Online Safety Act 2021 and the United Kingdom Online Safety Act 2023. The paper concludes that Malaysia should consider few highly effective initiatives impose in the Australian and the UK digital regimes including an integrated regulatory authority, risk assessments specific for children safety and stringent take down rules to be closer with international standards and practices in online child protection.

Keywords: cybersecurity laws, harmful content, Malaysia, online child safety, Online Safety Act

INTRODUCTION

The advanced technology using the Internet is a two edged sword presenting benefits and possible risks and threats for the children. This situation requires cybersecurity laws to act as a safety net in protecting child communications online. In response to this issue and other digital safety concerns, Malaysia launched few legislation in 2024 and 2025. The digital legal initiatives are Cyber Security Act 2024, Communications and Multimedia (Amendment) Act 2025, Online Safety Act 2025, Penal Code (Amendment) 2024 and Personal Data Protection (Amendment) Act 2024, to name a few. Ironically, while Malaysia is still strengthening the legal framework to address online child safety, shocking news made headline nationwide about a 14-year old student charged with the murder of a 16-year old female student at their school [16]. Amongst the contributing reasons stated are social media influence and emotional impulses.

Against this background, the paper aims to examine the newly introduced digital laws in promoting child safety in Malaysia. The paper also briefly analyses selected laws in other jurisdictions include the Australian Online Safety Act 2021, Online Safety Amendment (Social Media Minimum Age) Act 2024 and the United Kingdom Online Safety 2023. The current Malaysian legal framework collectively protects children's rights, safety and welfare is not discussed including Child Act 2001, Domestic Violence Act 1994, Anti-Trafficking in Persons and Anti-Smuggling Migrants Act 2007, Guardianship of Infant Act 1961, Sexual Offences Against Children Act 2017 and Penal Code.

Legal Initiatives

Malaysian Legal Reform

The year 2024 and 2025 marked a fundamental move for Malaysia, as substantial legal amendments reformed the media and telecommunications technology and digital sectors. The new important laws are Cyber Security

Act 2024, Data Sharing Act 2025, Malaysia Media Council Act 2025 and Online Safety Act 2025. Relevant existing legislation received changes include Communications and Multimedia Act 1998, Communications and Multimedia Commission Act 1998, Penal Code and Personal Data Protection Act 2010. Furthermore, the Communications and Multimedia (Licensing) Regulations 2000 is revised to impose licensing to Internet messaging service and social media providers.

These initiatives are intensified with the establishment of National Artificial Intelligence Office and National Guidelines on AI Governance and Ethics governing policies and regulations on artificial intelligence ('AI'). Whilst few of the legal changes directly impacted upon the promotion of online children safety, others affected the issues moderately and are given passing reference only.

The Cyber Security Act 2024 ('CSA') works at a macro level with significant features of the formation of the National Critical Information Infrastructure (NCII) which include three layers authorities with different roles and responsibilities of the National Cyber Security Committee, Chief Executive of National Cyber Security Agency (NACSA) and NCII Sector Lead [6]. Additionally, cybersecurity businesses and service providers must commit to stringent practices, risk assessments, prompt reporting and licensing requirements [5].

The Online Safety Act 2025 ("OSA") key features include establishment of an online safety committee and confers more powers upon the Malaysian Communications and Multimedia Commission to govern digital platforms and reinforce safeguards, particularly for protection of child online [9]. The OSA supplements the existing Child Act 2001 in protecting child safety. The OSA imposes duties upon social media platform providers referred to as Licensed Application Services Providers and Licensed Content Applications Service Providers to enhance platform safety, to protect children and to restraint access to harmful content with annual submission of digital safety plan. This is reflected in section 18 of the OSA creating a duty of care to protect online safety of child user. The Fourth Schedule lists of harmful content include content on child sexual abuse material as provided for under section 4 of the Sexual Offences against Children Act (SOACA) 2017 and content that may induce a child to cause harm to himself [14]. Thus, this move improves SOACA 2017 with well-defined provisions for sexual extortion of children and live-steaming of child sexual abuse. The child sexual abuse material and content related to financial fraud are proactively restricted as 'priority harmful content'. Additionally, there are duties to apply steps to mitigate risk of exposure to harmful content, duty to issue guidelines to user, duty to enable user to manage online safety, duty to make available mechanism for reporting harmful content, duty to make available mechanism for user assistance, duty to establish mechanism for making priority harmful content inaccessible and duty to prepare Online Safety Plan. In ensuring these duties enhance the accountability among service providers, 10 subsidiary regulations are in the pipeline to regulate online harm [10]. These duties provides user guidelines, reporting mechanisms and user assistance.

The Penal Code (Amendment) Act 2025 changes the criminal landscape to incorporate matters of bullying in any kind extensively including psychological and online bullying under sections 507B to 507G. Key amendments include offences of threatening, abusive or insulting words or communication causing harassment, distress, fear or alarm or likely to feel harassed, distressed, fear or alarmed by such words, communication or act and causing a person to believe that harm will be caused. This move echoed the government's promises to safeguard society, especially those who are at risk including children, teenagers and individuals experiencing mental harassment by bullies [3].

The Personal Data Protection (Amendment) Act 2024 have essentially changed the term 'data user' to 'data controller' similar with the international standard and the latter carries the duty to immediately inform the authority and affected individuals of any data breach. The amendments also transformed the compliance backdrop with the enhancement of the responsibilities of data processors to deal with personal data suffering loss, misused, unauthorised access and other risks and a mandatory data protection officer(s) appointment ensuring full observance of the Personal Data Protection Act ('PDPA'). The changes allowed data portability to assist transfer of data requested by individuals between service providers and subject to certain conditions data can be transferred cross-border as well as recognition of biometric data. Data privacy related to children handled by third party may fall under these amendments but does not provide a right of action in civil proceedings against the organisation, data controllers or data producers under the PDPA.

The Communications and Multimedia (Amendment) Act ('CMA') 2025 and the Malaysian Communications and Multimedia Commission (Amendment) Act (MCMCA) 2025 significantly enhanced the protection for individuals including children and increased the MCMC powers for non-compliance by the service providers. Key amendments related to child include expansion of section 233 of the CMA to insert the term 'grossly' as part of the offence which read "indecent, obscene, false, menacing or 'grossly' offensive" content and to incorporate new element of offence to the existing phrase of prohibited content an intent to "annoy, abuse, threaten or harass…" with the clause "or commit an offence involving fraud or dishonesty against any person"[4]. Additionally, six explanations are prescribed to elaborate content. They are obscene, indecent, false, menacing and grossly offensive content. Explanations of obscene, indecent and menacing content allocate special context related to child as stated in the following Table I.

Table I Explanations Of Content Related To Child

Type Of Content	Explanations
Obscene	In relation to a child, obscene content includes but not limited to child sexual grooming, sexual degradation that portrays any person as a mere sexual object or to demean the dignity, exploit or discriminate them, portrayal of sex or pornography including rape, attempted rape against child, sexual bestiality, whether consensual or otherwise.
Indecent	In relation to a child, indecent content includes but not limited to content which is profane in nature, improper and inappropriate for a child according to a reasonable adult's consideration.
Menacing	In relation to a child, menacing content includes but not limited to— (a) content that may cause emotional disturbance such as, portrayal of gruesome death, and domestic violence; or (b) content that may cause a child to imitate the portrayal of such act, such as content with suicidal tendencies, dangerous physical acts, street crime acts, or usage of drug.

Thus, these amendments strengthen measure to regulate prohibited content for children. The CMA also dedicated special punishment for offences in section 233 involving a child under eighteen years with penalty of RM500,000 and/or 5 years imprisonment and a further fine of RM5,000 for every day during which the offence is continued after conviction. Whilst new provision section 233A restraints sending of unsolicited commercial electronic message, new provision section 236A allows right of private action for network and fraud damage. Ironically on 19 August 2025 Malaysian court held that the words 'offensive' and 'annoy' under the previous scheme of section 233 of the CMA as unconstitutional as they are not line with Article 8 for equality and Article 10 for freedom of speech of the Federal Constitution. How far are the newly amended provisions considered as valid and the legal consequences upon child safety are yet to be tested in cases of future judicial review. The old regime of the CMA and MCMCA proven working with 1,521 cases of take down content considered as harmful or extremely harmful involving children by MCMC from 1st January 2022 to 15 October 2025 [10].

Australian Online Safety Act 2021

In 2015, Australia set a world precedent with the enactment of the Enhancing Online Safety Act 1915 and creation of an independent online regulator known as eSafety Commissioner (eSafety) [7]. The introduction of Australian Online Safety Act 2021 (AOSA) magnified the online safety landscape including digital child protection and abolished the old law. Essential features include enhancement of eSafety power, removal notice of cyber-abuse material targeted at an Australian adult and of intimate images without consent of a victim, and established 'class 1 material' hosted in Australia and 'class 2 material' hosted overseas. The AOSA coordinated these two classes of content with the National Classification Scheme that also regulate classifications of films, computer games and certain publications. Additionally, eSafety may request or require the internet service

providers to block material that depicts abhorrent violent conduct under the Criminal Code Act. Protection for children is highlighted in the following Table II [12].

Table Ii Highlights Of Protection For Children

TYPE	ACTION	CHILD RELATED ASPECT
Cyber-bullying material	Removal notice given to the provider of a social media service, relevant electronic service or designated internet service	The eSafety is satisfied that the material is or was cyber-bullying material targeted at an Australian child
Illegal and restricted material	Class 1 material include describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not)	Sexual exploitation of children. Child sexual exploitation material is any content that sexualises and takes unfair advantage of a child or young person under 18, as well as child sexual abuse material that shows their sexual assault.
Online Content Scheme	Declaration of a restricted access system by the eSafety	The objective is protecting children from exposure to material that is unsuitable for children. Restricted online content is material that is unsuitable for children, such as simulated sexual activity, nudity and high impact violence.
Social Media Minimum Age	Reasonable steps must be taken to prevent children who have not reached a minimum age from having accounts by social media platforms	There are privacy protections for information collected by social media platforms for the purposes of the minimum age requirement. An interference with the privacy of the individual for the purposes of the Privacy Act 1988.

The latest development is the passing of the Online Safety Amendment (Social Media Minimum Age) Act 2024 in November 2024. The Parliament strengthened the social media minimum age provision requesting the respective social media platforms to take reasonable steps to restrict Australian under 16 years old from having accounts starting from December 2025 [1].

The respective platforms are referred to as 'age-restricted social media platforms' providing services that satisfy the following conditions:

(i) the sole purpose, or a significant purpose, of the service is to enable online social interaction between 2 or more end-users;

(ii) the service allows end-users to link to, or interact with, some or all of the other end-users;

(iii) the service allows end-users to post material on the service.

Australian government have invested an amount $6.5 million for the Age Assurance Trial to commence the trial assessment of age verification, age estimation and other aspects incorporated across the digital system [1].

The UK Online Safety Act 2023

The UK Online Safety Act 2023 (UKOSA) primary aim is to protect children and adult online. The existing Office of Communications (Ofcom) is appointed as the independent regulator for the UKOSA [18]. The UKOSA imposes a variety of duties on the Internet service providers to regulate harmful and illegal content for online

children safety and to instigate schemes and methods to reduce risks for illegal activities on their platforms and remove the illegal materials [18]. Amongst the duties are to conduct a children's access assessment and duties to protect children's online safety. Services accessed by children are responsible to execute children's risk assessment, continuous monitoring and effectively managing measures to lessen the risk of children retrieving harmful content including changing algorithms and enforcing age verification [8].

Harmful content for children is classified into two types and further explained in the following Table III [13].

Table Iii Harmful Content For Children

DUTY	LEVEL OF RISK	
Children's risk assessment duties. A duty to carry out a suitable and sufficient children's risk assessment at a time specified in the UKOSA.	Primary Priority Content	Pornographic content. Content which encourages, promotes or provides instructions: for suicide or for an act of deliberate self-injury or for an eating disorder. (Section 61)
	Priority Content	Content which is abusive. Content which incites hatred against people. Content which encourages, promotes or provides instructions for an act of serious violence against a person. Bullying content. Content which depicts real serious violence against a person/animal or serious injury of a person/animal. Content which encourages, promotes or provides instructions for a challenge or dangerous stunt. Content which encourages a person to ingest, inject or inhale harmful substance. (Section 62)

Special highlights of harmful contents are a new criminal offence created for intentionally promoting or aiding serious self-harm and subjected any service that permit users to communicate material or interrelate with each other to provisions of the UKOSA. The duties compel the service to quickly withdraw unlawful suicide and self-harm material and actively safeguard users from material that is prohibited under the Suicide Act 1961 [18].

Analysis of the Legal Positions

The analysis focusses on three primary legislative moves include Malaysian legal reform, particularly the Online Safety Act 2025 (OSA), Australian Online Safety Act 2021 (AOSA), and the United Kingdom Online Safety Act 2023 (UKOSA). The main emphasis is on online child safety in underlining the parameter of the protection, responsibilities and implementation as summarised in the following Table IV.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue XI November 2025

Table Iv Comparative Outline

Country	Malaysia	Australia	The United Kingdom
Legislation	Legal Reform include the Online Safety Act 2025	The Online Safety Act 2021	The Online Safety Act 2023
Regulator	MCMC (PDP Commissioner for data and NCSA for cybersecurity)	eSafety Commissioner	Ofcom
Areas of Protection	Online protection duties for service providers (ASPs and CASPs) exclusive of cross-border application and private messaging	Private messaging, ISPs, app stores, search services, user-to-user, hosting; comprehensive industry codes	Search services connect to UK based content and user-to-user; classification limits for large services
Duty of Care	Child safety, protection instruments, support and reporting system, Online Safety Plan; MCMC profound jurisdiction	Online safety protections and expectations, binding industry codes, age assurance duties	Safety by design, child protection, children's risk assessments and safety codes, age verification duties
Age Assurance/ Verification	Not dictated across services; industry code contains child-specific measures, access control to priority harmful content	Detection/ removal available in the industry codes, age assurance and access control duties	Children's access assessments, age verification and access control to primary priority harms duties
Risk Assessments	Measure to mitigate risk, Online Safety Plan	Restricted access system, 24-hour removal notices	Illegal Content Risk Assessment (ICRA); Children's Access Assessment (CAA); Children's Risk Assessment (CRA)
Takedown Timeframe	No explicit 24-hour rule, MCMC can order fixed unavailability	24-hour removal duration for notices (expandable)	Necessary expeditious takedown; codes/guidance provide timing
Enforcement	Heavier penalties, audit, mandatory standards, regulate spams; network security measures	Availability of civil actions; blocking of offensive violent content	Criminal liability for senior managers; high punitive measures; business interruption orders
Search/ App Services Inclusion	Inclusion only of content/application services; licensing for large service providers	Inclusion of search and app services under the industry codes	Inclusion of search services; additional category duties
Coverage of Private Messaging	Not covered under the OSA	Covered under the industry codes	Covered (user-to-user services) and with duties

Malaysia has made significant moves with the Online Safety Act 2025, CMA (Amendment) Act 2025 and Cyber Security Act 2024. However, this initiative is less proactive, limited scope, and lacking in enforcement compared to legal positions in Australia and the UK. Based on Table IV, essential gaps in online child safety scheme involve at least five aspects, firstly, Malaysia's multiple agency scheme i.e. MCMC, National Cyber Security Agency

(NCSA), Online Safety Committee and PDP may decrease cohesive focus on children implementation compared to the UK's Ofcom and Australia's eSafety Commissioner as one entity regulators.

Secondly, no dictated age assurance and age based access control in Malaysia. Australia imposes age restriction under 16 years to register social media account and the UK enforces age assurance and age verification for services accessed by children. Nonetheless, on 23 November 2025, Malaysian Minister of Communications announced the plan to follow the Australian move with age assurance at 16 years and age verification using electronic know your customer (eKYC) application [17].

Thirdly, Malaysia's system is mostly complaint and direction driven and lacks current risk assessments (ICRA, CAA, CRA) and child safety codes apply in the UK. Australia implements proactive duties with strict removal order. On this note Malaysia promises 10 subsidiary regulations to regulate online harm with the hope that they will be at par with the international standards. Fourthly, enforcement disparity may exist although Malaysia introduced stronger audit and suspension powers with enhanced penalties under CMA (Amendment) 2025. Whilst Australia commands a 24-hour takedown rule, the UK imposes executive criminal liability.

Fifthly, private messaging is expressly excluded under the OSA although there are potential risks for grooming and exploitation, unlike inclusion of private messaging features in the Australia's broad industry codes and the UK's comprehensive user to user protection

RECOMMENDATIONS AND CONCLUSION

Proposed changes to the Malaysian online legal landscape include a stronger cross agency coordination between MCMC, NCSA, PDP and Online Safety Committee, not to mention the existence of a Chief Children's Commissioner created under the Human Rights Commission of Malaysia (SUHAKAM) (Amendment) Act 2023 and a possibility of a consolidated operative authority to head the child safety agenda. The suggested updates are enhancement of industry code for internet messaging or social media providers to request limitation of adult child interaction. The private messaging features may be incorporated into the OSA with privacy protection and encryption to lessen the risk for child grooming and exploitation.

Furthermore, the proposed shift is the adoption of the UK approach for age verification and restrain access for primary priority harmful content for services possibly accessed by children. The age assurance at 16 is in the pipeline and requires refined technical accuracy and reliability to implement in Malaysia with criteria closer to international standards. While Malaysia has an Online Safety Plan, the UK introduces 'living' risk assessments with child based context. Malaysia may consider to strengthen the online child safety with the UK specific approach, particularly Illegal Content Risk Assessment (ICRA), Children's Access Assessment (CAA), and Children's Risk Assessment (CRA).

Malaysia has made significant steps in online safety and digital control. To learn the lesson from the Australian and the UK scheme with proactive and highly effective enforcements, Malaysia may improve the current legal reform to enhance matters related to age assurance, private messaging, risk assessments, 24-hours takedown rule and consolidated enforcement authority. The moment of truth of the OSA 2025 will be subjected to MCMC's capacity to implement the new platform duties and the severity of the imposed penalty. The race with advanced technologies will always be a gap for digital literacy of the policy makers, enforcement agencies and parents. The broader definitions of 'harmful content' may open to argument against the right to freedom of speech and expression. Thus, the primary aspiration is to transform the digital environment into a safe place for children using the technology and internet.

ACKNOWLEDGMENT

The authors are thankful to the Faculty of Law, Universiti Teknologi MARA, Shah Alam, Malaysia. for supporting the research activities.

REFERENCES

1. Australia Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, (2025). Current Legislation. Retrieved from https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation.
2. BBC, (24 July 2025). What the Online Safety Act is - and how to keep children safe online. Retrieve from https://www.bbc.com/news/articles/c0epennv98lo.
3. Bernama, (11 July 2025). Heavier penalties for doxing, stalking, mental harassment as anti-bullying law takes effect. (11 July 2025). New Straits Times: Malaysia. Retrieved from https://www.nst.com.my/news/nation/2025/07/1243456/heavier-penalties-doxing-stalking-mental-harassment-anti-bullying-law.
4. Christopher and Lee Ong, (2025). An Overview of Key Changes Introduced by the CMA Amendment Bill. Malaysia. Retrieved from https://www.christopherleeong.com/wp-content/uploads/2025/01/2025-01_An-Overview-of-Key-Changes-Introduced-by-the-CMA-Amendment-Bill.pdf.
5. Clarence Chan, (2024). PricewaterhouseCoopers Malaysia: Cyber Security Act 2024 – A New Era for Cybersecurity in Malaysia. Retrieved from https://www.pwc.com/my/en/assets/publications/2024/pwc-my-cyber-security-act-2024-new-era-for-cybersecurity-in-malaysia.pdf.
6. Digital News Asia, (3 March 2025). Malaysia's Cyber Security Act 2024 (Act 854): Building Trust and Seizing Global Opportunities. Retrieved from https://www.digitalnewsasia.com/business/malaysias-.
7. eSafety Commissioner, (2025). Learn About the Online Safety Act. Retrieved from https://www.esafety.gov.au/newsroom/whats-on/online-safety-act.
8. Latham and Watkins, (2024). UK Online Safety Act 2023. Retrieved fromhttps://www.lw.com/admin/upload/SiteAttachments/UK-Online-Safety-Act-2023.pdf.
9. Malay Mail, (16 June 2025). Azalina: Online Safety Act coming into force soon, targets digital harm to children. Malaysia. Retrieved from https://www.malaymail.com/news/malaysia/2025/06/16/azalina-online-safety-act-coming-into-force-soon-targets-digital-harm-to-children/180552.
10. Mohamad Al As, Nor Ain Mohamad Radhi. (3 November 2025). MCMC drafting 10 subsidiary laws under Online Safety Act – Fahmi. New Straits Times: Malaysia. Retrieved from https://www.nst.com.my/news/nation/2025/11/1307634/mcmc-drafting-10-subsidiary-laws-under-online-safety-act-fahmi.
11. Nathaniel Amos, (5 May, 2023). What is Ofcom and what does it do?. Institute for Government: the United Kingdom. Retrieved from https://www.instituteforgovernment.org.uk/explainer/ofcom.
12. Online Safety Act 2021 (Australia). Retrieved from https://www.legislation.gov.au/C2021A00076/latest/text.
13. Online Safety Act 2023 (UK). Retrieved from https://www.legislation.gov.uk/ukpga/2023/50/section/62.
14. Online Safety Act 2025 (Malaysia). Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/Online-Safety-Act-2025-Act-866.pdf.
15. Parliament of Australia, (21 August 2024). Research Paper: Children, online safety, and age verification. Retrieved from https://www.aph.gov.au/About_Parliament/ Parliamentary departments/Parliamentary_Library/Research/Research_Papers/2024-25/Children_online_safety.
16. Teh Athira Yusof, (22 October 2025). Teen charged with murder of student at Bandar Utama school. The Star: Malaysia. Retrieve from https://www.thestar.com.my/news/nation/2025/10/22/teen-charged-with-murder-of-student-at-bandar-utama-school.
17. The Straits Times. (2025). Malaysia to implement social media ban for teens under 16. Retrieved from https://www.straitstimes.com/asia/se-asia/malaysia-to-implement-social-media-ban-for-teens-under-16.
18. The United Kingdom Government, Department for Science, Innovation and Technology. (2025). Guidance: Online Safety Act. Retrieved from https://www.gov.uk/government/collections/online-safety-act.