|  |  |
| --- | --- |
|  | **Document CWG-COP-23/INF/6** |
| **4 September 2025** |
| **English only** |
|  |  |
| Contribution by Malaysia | |
| CURRENT AND FORTHCOMING MEASURES TO ADDRESS CHILD ONLINE EXPLOITATION THROUGH THE NATIONAL ONLINE SAFETY FRAMEWORK | |
| **Purpose**  The purpose of this document is to present Malaysia’s current frameworks and initiatives for the protection of children from online exploitation and to introduce the forthcoming National Online Safety Framework (NOSF) as a holistic, three-pronged approach encompassing Regulatory, Awareness and Collaboration pillars. NOSF is currently in development, it is intended to serve as a strategic blueprint to strengthen national efforts and foster a safe, secure and inclusive online environment.  This contribution is provided to the Council Working Group on Child Online Protection in line with Resolution 179 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, which emphasises the important role of the ITU in facilitating international collaboration on child online protection.  **Action required**  This report is transmitted to the Council Working Group on child online protection **for information**.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **References**  *Resolution* [*179 (Rev. Bucharest, 2022)*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-179-E.pdf) *of the Plenipotentiary Conference on ITU's role in child online protection.* | |

1. **Introduction**

According to the UNICEF Malaysia Annual Report 2024[[1]](#footnote-1), one in every 25 children aged between 12 to 17 is subjected to online sexual exploitation and abuse (OCSEA) annually. Under Section 2(1) of the Child Act 2001, a “child” is defined as a person below the age of 18. This vulnerable demographic represents approximately 9.14 million individuals, accounting for 26.9% of Malaysia’s total population of 34.06 million (Department of Statistics Malaysia, 2024).

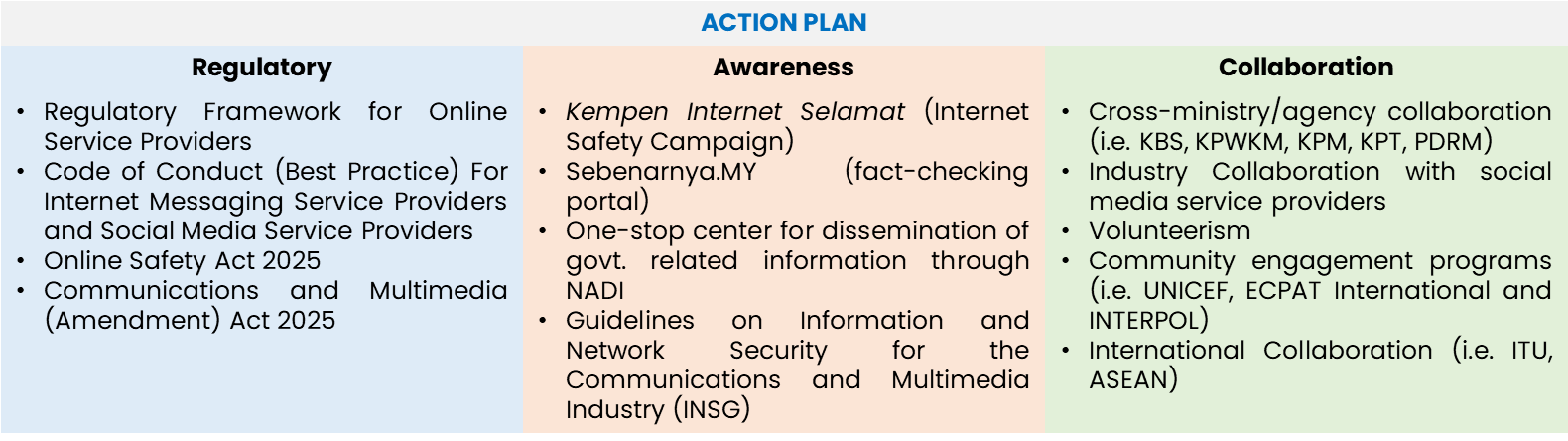
The rapid growth of digital connectivity has fundamentally changed the way children interact with the world. While it has created opportunities for learning and social connection, it has also exposed children to new risks. The Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (2nd Edition)[[2]](#footnote-2) highlight that exploitation may occur not only through physical threats or force but also through manipulation, deception, online grooming and power imbalances. These risks are amplified by the easy accessibility of harmful content, the anonymity of online spaces and the sophistication of digital tools that can be misused by offenders.

The impact of online exploitation is profound and long lasting. Victims may experience emotional trauma, a loss of trust in adults and difficulties with personal relationships, all of which can persist into adulthood. Without strong preventive and protective systems, children can become desensitized to harmful behaviours and increasingly vulnerable to exploitation.

To address the challenges of child online exploitation and other online harms, NOSF is envisioned as a strategic initiative led by the Malaysian Communications and Multimedia Commission (MCMC). The framework aims to strengthen Malaysia’s overall approach to online safety, with a particular focus on children, family and other vulnerable populations. In response to the growing threats of cyberbullying, online fraud, hate speech, and exploitation, NOSF serves as a national blueprint for coordinated, comprehensive, and future-facing responses to online harms.

The vision of NOSF is to provide a unified strategic direction for online safety efforts across all sectors, while its mission is centred on establishing a coordinated approach to combating online harms, promoting responsible digital behaviour, and creating a safe, inclusive, and resilient online environment for all Malaysians.

NOSF is built on three key objectives. First, it seeks to strengthen regulatory frameworks to enhance protection against online risks. Second, it aims to promote targeted education and awareness initiatives to help users better understand and respond to online harms. Third, it emphasises the importance of building strategic partnerships with stakeholders across government, industry, and civil society to address evolving challenges in the digital space effectively.



The framework continues to evolve through ongoing consultation and collaboration with relevant stakeholders. NOSF is expected to set a national model for online safety that reflects Malaysia’s digital priorities and broader social values.

**2.0 Regulatory**

Malaysia, through the MCMC, has developed regulatory measures that provide the legal foundation for preventing, detecting and responding to child online exploitation. These measures include targeted legislation, licensing obligations for online service providers and enforceable codes of conduct. Collectively, they form the first prong of the NOSF, aimed at safeguarding children in the digital environment.

Beyond NOSF, Malaysia is also strengthening broader child rights governance through the establishment of the Office of the Children’s Commissioner under the Human Rights Commission of Malaysia (SUHAKAM) and the drafting of a Children’s Commission Bill. This forthcoming institution is envisioned as a cornerstone of child rights protection, creating an independent statutory body with authority to monitor compliance, investigate complaints, advocate for policy reforms and ensure that children’s voices are meaningfully represented in national policymaking.

**2.1 Regulatory Framework for Online Service Providers**

The MCMC has adopted a targeted and proportionate approach to regulating online services, with a focus on Internet messaging and social media platforms that have a significant user base in Malaysia.

The regulatory framework applies exclusively to two categories of online services that meet the established threshold of eight (8) million or more users in Malaysia:

* Internet Messaging Platforms, such as WhatsApp, Telegram, and WeChat; and
* Social Media Platforms, such as Facebook, Instagram, TikTok, and YouTube.

The threshold ensures that regulatory attention is directed toward platforms with substantial influence in the Malaysian online space, while excluding smaller platforms to maintain proportionality and operational practicality.

The regulatory framework was gazetted on 1 August 2024 and came into effect on 1 January 2025, following amendments to the:

* Communications and Multimedia (Licensing) Regulations 2000, and
* Communications and Multimedia (Licensing) (Exemption) Order 2000.

The aim of this regulatory framework is to ensure that major online service providers are held accountable for managing illegal and harmful content and are subject to Malaysian laws to uphold user safety and platform integrity.

This measured approach allows the Government of Malaysia to safeguard users from online harm, while continuing to support innovation and growth in the online services ecosystem.

**2.2 Code of Conduct (Best Practice) For Internet Messaging Service Providers and Social Media Service Providers**

To strengthen platform accountability and promote safer online spaces, the MCMC developed a Code of Conduct (Best Practice) for Internet messaging and social media service providers. This Code sets out best practices for addressing harmful content in alignment with the Communications and Multimedia Act 1998 (CMA 1998) and other relevant Malaysian laws.

The Code was developed through a series of workshops, engagement sessions, and a public consultation process. It was officially published on 20 December 2024 and is now publicly available on the MCMC’s official website.

The main objective of the Code is to support the broader regulatory framework by providing clear conduct expectations for licensed service providers, particularly with regard to managing and mitigating harmful content. In doing so, the Code aims to enhance online safety and digital well-being, especially for children and vulnerable groups.

Service providers are recommended to take effective action against a range of harmful content, including:

* Child Sexual Abuse Material (CSAM)
* Non-consensual sharing of intimate content
* Content related to online scams, including phishing, romance scams, and investment fraud
* Bullying and harassment
* Content inciting violence, extremism, or terrorism
* Content likely to induce self-harm, especially among children
* Hate speech
* Promotion of illegal drug use
* Manipulated or deceptive media, such as deepfakes

By addressing these risks, the Code promotes accountability and responsibility on the part of the service providers to implement meaningful safeguards, uphold community standards, and contribute to a safer and more secure online environment.

**2.3 Online Safety Act 2025**

The Online Safety Act 2025 (ONSA 2025) was gazetted on 22 May 2025 and will be enforced in due course. ONSA 2025 introduces a comprehensive legal framework to enhance and promote online safety in Malaysia by regulating harmful content and establishing clear duties and obligations for Application Service Providers (ASPs), Content Application Service Providers (CASPs), and Network Service Providers (NSPs), who are licensed (service providers). It is designed to promote a safer and more accountable digital ecosystem, with a strong emphasis on protecting children, families, and other vulnerable groups.

ONSA 2025 empowers the MCMC to set clear expectations for service providers in safeguarding users, promoting accountability, and building public trust. The subsidiary legislations for ONSA 2025 which are been developed will ensure effective implementation measures and duties of service providers against online harms. These subsidiary legislations will address key areas such as child online protection, risk mitigation, content moderation, and platform governance. One such requirement is the Online Safety Plan, which service providers must prepare and publish to demonstrate how they manage risks, comply with their legal obligations, and protect users particularly children.

Where providers fail to meet these obligations, MCMC is empowered to take enforcement action, including the imposition of substantial penalties and cooperation with law enforcement authorities.

**2.4 Communications and Multimedia (Amendment) Act 2025**

The Communications and Multimedia (Amendment) Act 2025 came into force on 11 February 2025, following its gazettement on 7 February 2025. These amendments mark a significant step toward creating a more secure and sustainable internet ecosystem, with a particular emphasis on enhancing user protection, especially for children and families.

Among the key changes is the strengthened regulation of online content under Section 233, where the legal interpretation of content and intent behind postings has been further refined. The scope has also been expanded to include content related to fraud and dishonesty, significantly enhancing the legal tools available to combat scams, financial deception, and online harms against children.

Further, to complement these measures, Section 211A has been introduced to authorise MCMC to suspend services that violate legal content requirements, providing an additional layer of enforcement to ensure compliance with Malaysian laws.

**3.0 Awareness**

As part of Malaysia’s contribution under the NOSF, building public awareness is recognised as a critical pillar that complements legal and regulatory measures in addressing child online exploitation. Awareness initiatives are designed to empower children, parents, educators and the wider community with the knowledge and skills to navigate digital spaces safely.

A notable initiative is the #OnlineSafetyIRL Youth Fellowship[[3]](#footnote-3), a two-month programme that aims to empower youth leaders as advocates and policy influencers in digital safety. Participants aged 18 to 25 undergo a structured curriculum, beginning with an in-person induction, followed by a comprehensive series of masterclasses covering topics such as online safety and scam prevention, digital literacy and fact-checking, public speaking, and policy-making principles. Fellows then participate in an immersive learning week, where they experience policy-making in action through field visits. The programme concludes with fellows crafting policy proposals through action-plan development, enabling them to contribute meaningfully to shaping safer digital policies.

This fellowship underscores the significance of youth participation in digital policymaking and reinforces Malaysia’s child-centred awareness strategy under the NOSF. By empowering young leaders to champion safer digital practices, it complements broader national awareness efforts and demonstrates the value of engaging different segments of society in shaping online safety.

In parallel, Malaysia, through MCMC, has implemented nationwide awareness campaigns and digital safety platforms that extend the reach of online safety education to schools, families and the wider public. Together, these initiatives ensure that awareness remains a cornerstone of Malaysia’s national strategy under the NOSF.

**3.1 *Kempen Internet Selamat* (Internet Safety Campaign)**

The *Kempen Internet Selamat* (KIS) was introduced as a nationwide campaign to raise awareness of internet safety, with a particular emphasis on school students and families. The initiative directly addresses critical online harms such as scams, cyberbullying, online gambling, inappropriate social media use by underaged users and the exploitation and sexual abuse of children. By embedding these themes into its modules, KIS strengthens Malaysia’s preventive approach to child online exploitation and aligns with the broader objectives of NOSF.

KIS has progressively expanded from schools to higher education institutions and into the wider community, reflecting Malaysia’s whole-of-society approach to online safety. The campaign is implemented through close collaboration with government agencies, associations, non-governmental organisations and the private sector, while also leveraging media publicity and nationwide outreach to ensure visibility.

KIS is delivered and assessed through interactive methods such as facilitators’ observations, reflection sessions and quizzes during activities. To ensure effectiveness, the learning modules are stratified by age category. For children aged seven to twelve, modules focus on recognising good versus harmful content, understanding rights and responsibilities, adhering to social media age restrictions, and identifying types of online harms such as cyberbullying, hate speech and sexual exploitation. For adolescents aged thirteen to seventeen, the curriculum addresses digital reputation, misinformation and sexual exploitation. Youth modules emphasise online fraud, cyberbullying and oversharing, while modules for adults and senior citizens build capacity on digital literacy, hate speech, artificial intelligence and deepfakes, online fraud and collective responsibility in maintaining online safety.

As of 1 August 2025, KIS has been implemented in 612 schools and higher education institutions under the Ministry of Education and Ministry of Higher Education, reaching over 60,000 participants, while broader community outreach has engaged more than 160,000 participants through 167 programmes. With an ambitious target of reaching 8,000 schools nationwide by December 2025, KIS continues to serve as a cornerstone of Malaysia’s national awareness-raising strategy under NOSF, contributing to the creation of a safe, responsible and child-centred digital ecosystem.

The success of KIS builds on the legacy of *Klik Dengan Bijak* (KDB), which was launched by MCMC in 2012 as one of Malaysia’s earliest nationwide internet safety awareness initiatives. KDB promoted safe and ethical digital practices through workshops, school training, community roadshows and social media engagement. Its impact was recognised internationally when it was named a WSIS Prize Champion in 2020 under the “Ethical Dimensions of the Information Society” category and selected as a WSIS Forum Photo Contest Winner in 2023, while also being recognised as a nominated project in the same “Ethical Dimensions of the Information Society” category. Although KDB is no longer active as a standalone programme, its legacy demonstrates Malaysia’s longstanding commitment to digital literacy and continues to inspire KIS as the flagship national awareness campaign under the NOSF.

**3.2 Sebenarnya.MY (fact-checking portal)**

Since its launch in 2017, Sebenarnya.MY has been Malaysia’s central fact checking portal. It provides the public with a trusted platform to verify unverified news and to curb the spread of misinformation. Beyond verification, the portal educates the public on how to recognise false information by offering practical tips. These tips include verifying sources, cross checking dates and carefully evaluating images or videos that may have been manipulated.

Building on this foundation, MCMC introduced the Chatbot Sebenarnya.MY in January 2025. It is also known as the Artificial Intelligence Fact Check Assistant (AIFA). This tool enhances the portal’s functionality by using artificial intelligence and machine learning. It enables users to verify information quickly and easily through the portal and through WhatsApp. AIFA provides real time fact checking, educates users on identifying credible sources and encourages community participation in reporting false content. It is available in several languages including Bahasa Melayu, English, Chinese and Tamil. This ensures inclusivity across Malaysia’s diverse population.

The deployment of AIFA reflects Malaysia’s proactive response to evolving digital risks, especially misinformation that can create fear, division or confusion online. By strengthening public media literacy and offering accessible fact checking tools, Sebenarnya.MY and AIFA directly support the Awareness pillar of the NOSF. Together, these initiatives reduce the harmful impact of misinformation, promote responsible online engagement and protect children and young users by ensuring that their online environment is shaped by verified and credible information.

**3.3 National Information Dissemination Centre (NADI)**

The National Information Dissemination Centres (NADI), established by MCMC under the Universal Service Provision (USP), provide shared internet access to empower communities, particularly in rural and underserved areas. By offering collective connectivity, NADI enables communities to explore new opportunities while strengthening their digital resilience. The introduction of NADI Smart Services in July 2024 further elevated digital literacy and improved the quality of life for Malaysians, especially those in areas with limited access.

As of mid-2025, NADI has achieved notable progress. A total of 1,098 centres are operational nationwide (as of July 2025), with 1.7 million registered members (as of June 2025). Participation in NADI Smart Services has reached 623,315 individuals and 9,337 participants have benefitted from entrepreneurship programmes delivered through NADI. These achievements highlight NADI’s role in bridging the digital divide, fostering socio-economic empowerment and expanding opportunities for vulnerable groups, including children.

International recognition has reinforced NADI’s contribution to safe digital participation. In 2025, NADI was awarded WSIS Champion in Action Line C4 (Capacity Building), underscoring its success in advancing community-based digital literacy and resilience. Importantly, NADI aligns with the Awareness pillar of the NOSF by equipping children, parents and educators with the knowledge and skills to navigate digital spaces responsibly. This alignment strengthens Malaysia’s broader efforts to combat OCSEA by ensuring that awareness and capacity-building initiatives complement the country’s legal, regulatory and enforcement measures.

**3.4 Guidelines on Information and Network Security for the Communications and Multimedia Industry (INSG)**

As part of Malaysia’s current and forthcoming measures under the NOSF, the Information and Network Security Guidelines (INSG) represent a proactive step toward safeguarding children online through strengthened cybersecurity measures. The INSG was officially introduced to the public on 8 December 2024 by MCMC. It serves as a voluntary, best-practice framework for service providers under the CMA 1998, designed to enhance their cybersecurity readiness without imposing new regulations.

The INSG aims to strengthen the capacity of service providers to manage risks, mitigate data breaches and minimise disruptions through resilient networks and infrastructures. It also defines clear roles and accountabilities to protect consumer interests, uphold national security and foster public trust. By offering comprehensive guidance on cybersecurity measures across network infrastructures and the wider communications supply chain, the INSG helps ensure the protection of user rights and privacy. Importantly, it supports efforts to address emerging threats such as ransomware, distributed denial-of-service (DDoS) attacks, scams, child sexual abuse material, cyberbullying and other forms of online harm.

The guidelines were developed through an inclusive consultation process that engaged cybersecurity firms, government agencies, NGOs, academia, licensees and industry players such as data centres and cloud service providers. While applicable to all designated service providers under the CMA 1998, the INSG allows exemptions at the discretion of MCMC for providers that submit written requests, with the Commission determining the scope, conditions and duration of such exemptions.

By embedding cybersecurity best practices that strengthen defences against online harms, including those that target children, the INSG complements Malaysia’s wider regulatory and awareness initiatives under the NOSF. It reflects the government’s commitment to creating a safer and more resilient digital ecosystem where online safety and child protection are integral to the nation’s cybersecurity agenda.

The INSG operates alongside existing legislation, including the CMA 1998, the Digital Signature Act 1997, the Personal Data Protection Act 2010, the Cyber Security Act 2024 and any future statutes or regulatory instruments issued by MCMC. Where stricter requirements are prescribed under other applicable laws, those provisions take precedence over the INSG.

**4.0 Collaboration**

Under the NOSF, collaboration is identified as a key pillar in Malaysia’s strategy to combat child online exploitation, with MCMC playing a coordinating and leadership role. By embedding partnerships across ministries, communities, industry and international agencies, MCMC ensures that Malaysia’s current and forthcoming measures are both nationally integrated and globally relevant.

**4.1 Cross-Ministry and Agency Collaboration**

Malaysia has institutionalised cross-ministerial cooperation as part of the NOSF to ensure that child protection responsibilities are mainstreamed across all relevant agencies. Ministries such as the Ministry of Youth and Sports (KBS), the Ministry of Women, Family and Community Development (KPWKM), the Ministry of Education (KPM) and the Ministry of Higher Education (KPT) coordinate policies and programmes to address online risks faced by children. For example, MCMC collaborates with the Royal Malaysia Police (PDRM) on special operations to address online exploitation. These joint efforts have led to prompt investigations, the seizure of harmful material and the arrest of offenders, making online spaces safer for children.

**4.2 Industry Collaboration with social media service providers**

Collaboration with social media service providers is central to Malaysia’s NOSF, particularly in safeguarding children from harmful online content. MCMC has worked with platforms such as TikTok, Meta and Telegram to ensure compliance with national laws and platform community standards. Between January 2022 and August 2025, more than 500,000 items of harmful content were removed following MCMC’s intervention, including posts related to scams, fraud, obscene material, cyberbullying and misinformation.

TikTok has been a focal point of regulatory engagement. In 2023, MCMC issued nearly 1,900 removal requests to the platform, the highest globally for a single region, reflecting the scale of collaboration. While TikTok clarified that it does not act on government directives alone, it confirmed that it works with regulators like MCMC and proactively removed almost 1,000 harmful videos in a single week. In early 2025, MCMC also raised concerns with TikTok over the unexplained blocking of 18 Malaysian media accounts, reinforcing its role in protecting both online safety and media freedom.

Beyond enforcement, MCMC has expanded its partnerships to include technology companies that can strengthen digital resilience. In July 2024, MCMC signed a memorandum of understanding with Microsoft Malaysia to launch the AI TEACH programme. The initiative aims to enhance digital and artificial intelligence literacy among vulnerable communities, especially those near NADI. Training modules cover generative artificial intelligence, employability skills and ethical artificial intelligence use, with participants learning practical applications through tools such as Microsoft Copilot.

Through these combined efforts with global platforms and technology partners, Malaysia demonstrates a balanced and forward-looking approach to industry collaboration. The strategy integrates regulatory enforcement, constructive engagement with service providers and innovation-driven capacity building, ensuring that child protection remains at the centre of the NOSF.

**4.3 Volunteerism**

Volunteerism plays a vital role in Malaysia’s collaborative strategy under the NOSF by embedding online safety and digital literacy at the community level. A key initiative is the Malaysia ICT Volunteer (MIV) programme, coordinated by MCMC. Established in 2016, the MIV programme serves as an empowerment platform to enhance and sustain digital literacy nationwide, bridging the digital divide one community at a time. Guided by its motto Learn, Enjoy, Serve, Respect, the initiative nurtures responsible, ethical and competent digital citizens who actively contribute to safer digital environments.

The MIV programme mobilises volunteers including youth, women, retirees, educators and community leaders to support information and communications technology projects that promote online safety, prevent cyberbullying, reduce online fraud and strengthen child protection. It has also developed community-based digital leaders by equipping them with the skills to create applications, digital content and services tailored to local needs.

By 2024, more than 11,300 volunteers had been recruited and trained nationwide. These included teachers, higher education students and community members, ensuring outreach to both urban and rural populations. In 2023 alone, nearly 500 MIV programmes reached over 2.3 million people with volunteers supporting awareness campaigns that reinforced responsible and secure online behaviour.

Through this model of community-driven volunteerism, the MIV programme reflects Malaysia’s whole of society approach under the NOSF. It ensures that digital literacy, online safety and protection against child online exploitation are promoted by communities for communities.

**4.4 Community Engagement**

Malaysia further strengthened its child protection strategies by participating in the Disrupting Harm[[4]](#footnote-4) initiative in 2022. Jointly conducted by UNICEF, ECPAT International and INTERPOL, this regional research effort examined the prevalence and nature of online child sexual exploitation and abuse in thirteen countries. The findings revealed that approximately 100,000 children in Malaysia aged 12 to 17 had been subjected to online exploitation. The study identified stigma and a lack of awareness about reporting mechanisms as key barriers to justice. In response, Malaysia convened a national consultation co-organised by UNICEF and the Ministry of Women, Family and Community Development. Supported by MCMC and civil society organisations, the dialogue generated policy recommendations focused on strengthening education, simplifying child reporting procedures and improving multisectoral coordination. Malaysia’s active engagement in this initiative highlights its commitment to applying data-driven approaches and international good practices in national reform.

**4.5 International Collaboration**

Malaysia’s contribution to addressing child online exploitation under the NOSF is significantly reinforced through international collaboration and regional leadership. These efforts underscore the nation’s strategic role in shaping policies and frameworks to safeguard children online.

Malaysia first demonstrated international leadership when it hosted the International Multilateral Partnership Against Cyber Threats (IMPACT)[[5]](#footnote-5) in Cyberjaya in 2008. As the operational home of the ITU’s Global Cybersecurity Agenda, IMPACT provided technical cooperation, capacity building, and child protection resources to ITU Member States. Although IMPACT no longer operates in its original structure, Malaysia’s early support reflects a long-standing commitment to global cybersecurity and child protection.

Malaysia’s continuing engagement with the ITU is evident in its role as Vice-Chair of the ITU CWG‑COP. Malaysia has significantly contributed to the development of the ITU Guidelines on Child Online Protection, which remain central to guiding Member States, educators, and industry in establishing safer online environments.

At the regional level, Malaysia actively participates in the ASEAN Digital Ministers Meetings (ADGMIN) and other ICT platforms focusing on children’s digital rights, responsible development, and platform governance. A major milestone was Malaysia’s endorsement of the ASEAN Declaration on the Protection of Children from All Forms of Online Exploitation and Abuse, adopted in 2019, and the subsequent ASEAN Regional Plan of Action (2021–2025), which Malaysia helped operationalise with commitments to enhance legislation, law enforcement, child support services, and private sector collaboration.

Malaysia is also leading the ongoing development of the Guidelines for the Safe and Responsible Use of Social Media Platforms for ASEAN, which aim to promote a safer, more inclusive and accountable digital environment across the region. These guidelines encourage responsible behaviour, digital literacy and awareness to minimise online risks, while fostering regional cooperation on online safety. Structured around four pillars which are regulatory, education and awareness, collaboration and sustainability and adaptability, the initiative reflects ASEAN’s collective commitment to resilience and mutual respect in the digital sphere.

True to its child-centred approach, Malaysia also engaged directly with children and youth during regional consultations across ASEAN, contributing to the Call to Action from Children and Young People to the Private Sector on Child Online Protection[[6]](#footnote-6). This advocacy document, shaped by young voices, enhanced Malaysia’s regional policy alignment by securing child input into the ASEAN Plan of Action.

**5.0 Conclusion**

Malaysia’s contribution to addressing child online exploitation is anchored in a comprehensive and forward-looking approach under NOSF. Through its three pillars, which are Regulatory, Awareness and Collaboration, the framework consolidates Malaysia’s current initiatives while introducing forthcoming measures to create a safer, more inclusive and child centred digital environment.

On the regulatory front, Malaysia has significantly strengthened its legal and institutional regulatory framework to address child online exploitation. The introduction of the Regulatory Framework and Code of Conduct for online service providers, the gazettement of the Online Safety Act 2025, and the recent amendments to the Communications and Multimedia Act 1998 provide clearer definitions of harmful content, mandate online safety plans, and introduce enhanced enforcement tools. These measures establish enforceable duties for service providers, raise accountability standards, and reinforce protections for children across digital platforms. Collectively, they mark a critical step towards ensuring that children are systematically safeguarded in the online environment.

The Awareness pillar complements legal measures by empowering children, parents, educators and communities through targeted programmes. Initiatives such as the *Kempen Internet Selamat*, Sebenarnya.MY and NADI have expanded outreach and strengthened digital literacy, with international recognition highlighting their impact. At the same time, the Information and Network Security Guidelines extend awareness to industry stakeholders, embedding best practices to address threats such as scams, cyberbullying and child sexual abuse material. Together, these efforts make awareness multidimensional, reaching both communities and service providers.

The collaboration pillar remains central to Malaysia’s strategy, uniting ministries, law enforcement, industry, civil society and international partners in a whole-of-government and whole-of-society approach. Cross-ministry cooperation, including joint efforts between MCMC and PDRM, has strengthened responses to online exploitation. Partnerships with platforms such as TikTok, Meta and Microsoft have enabled large-scale removals of harmful content and introduced initiatives like AI TEACH to build digital resilience. Volunteer-driven efforts through the MIV programme have empowered over 11,000 volunteers to promote digital literacy and online safety, reaching millions nationwide. Malaysia’s participation in the UNICEF-led Disrupting Harm study has ensured reforms are data-driven, while internationally, its leadership as Vice-Chair of the ITU CWG-COP, support for the ASEAN Declaration and Regional Plan of Action and ongoing role in developing the ASEAN Guidelines for the Safe and Responsible Use of Social Media Platforms reinforce its long-standing commitment to child online protection.

In conclusion, Malaysia’s current and forthcoming measures demonstrate a strong alignment with Resolution 179 of the Plenipotentiary Conference in Bucharest in 2022, which calls on Member States to exchange information on the current state of legislative, organisational and technical measures in the area of child online protection. By advancing the NOSF as a strategic blueprint, Malaysia underscores its commitment to ensuring that children can thrive in a safe, secure and inclusive digital ecosystem, while contributing to the shared global responsibility of protecting children online.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. <https://open.unicef.org/download-pdf?country-name=Malaysia&year=2024> [↑](#footnote-ref-1)
2. <https://ecpat.org/wp-content/uploads/2025/04/Second-Edition-Terminology-Guidelines-final.pdf> [↑](#footnote-ref-2)
3. [Youths IRL](https://www.onlinesafetyirl.com/youths-irl) [↑](#footnote-ref-3)
4. [Disrupting Harm: Malaysia](https://ecpat.org/wp-content/uploads/2022/09/DH_Malaysia_ONLINE_FINAL-1.pdf) [↑](#footnote-ref-4)
5. [ITU: Committed to connecting the world](https://www.bing.com/ck/a?!&&p=9d34bd29f6bfaeacde650a6c7a5a589d00a68db37a9cab10892c6b0d4b5765d2JmltdHM9MTc1NDQzODQwMA&ptn=3&ver=2&hsh=4&fclid=0dbd6830-b4f6-63ce-084f-7decb5616270&psq=host+of+the+ITU%e2%80%99s+IMPACT+cybersecurity+centre&u=a1aHR0cHM6Ly93d3cuaXR1LmludC9JVFUtRC9jeWIvY3liZXJzZWN1cml0eS9kb2NzL0lUVV9JTVBBQ1RfaW5mb3BhY2tfLnBkZg&ntb=1) [↑](#footnote-ref-5)
6. [A Call to Action from Children and Young People to the Private Sector on Child Online Protection](https://www.unicef.org/eap/media/12051/file/A%20Call%20to%20Action%20from%20Children%20and%20Young%20People%20.pdf) [↑](#footnote-ref-6)