|  |  |
| --- | --- |
|  | **Document CWG-COP-23/4** |
| **1 September 2025** |
| **English only** |
|  |  |
| **ITU-T Study Group 17** |
| LIAISON STATEMENT ON SG17 UPDATE ON THE WORK OF THE CORRESPONDENCE GROUP ON CHILD ONLINE PROTECTION (CG-COP) |
| **Purpose**This Liaison Statement informs Council Working Group on Child Online Protection (CWG-COP) of the progress of the CG-COP as reported at the meeting of the ITU-T Study Group 17 (Geneva, 8 - 17 April 2025), and it includes in annex the report on Gap analysis on standards that support child online protection (COP).**Action required**The Council Working Group on child online protection **is invited to note** this Liaison Statement and its report in [Annex](#Annex).\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**References**[*CWG-COP website*](https://www.itu.int/en/council/cwg-cop/Pages/default.aspx)*;* [*SG17-TD87/PLEN*](https://www.itu.int/md/T25-SG17-250408-TD-PLEN-0087/en)*,* [*SG17-TD42/PLEN*](https://www.itu.int/md/T25-SG17-250408-TD-PLEN-0042/en) |

|  |  |  |
| --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2025-2028 | SG17-LS30 |
| **STUDY GROUP 17** |
| **Original: English** |
| **Question(s):** | 1/17, 10/17 | Geneva, 8-17 April 2025 |
| **Ref.:** [**SG17-TD87/PLEN**](https://www.itu.int/md/T25-SG17-250408-TD-PLEN-0087/en) |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on update on the work of the Correspondence Group on Child online protection (CG-COP) |
|

|  |
| --- |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For information to:** | CWG-COP, ITU-D Q3/2, ITU-D Q6/1, ISO/IEC JTC 1 SC 27/WG 5 |
| **Approval:** | ITU-T Study Group 17 meeting (Geneva, 17 April 2025) |
| **Deadline:** | - |

 |
| **Contact:** | Arnaud TADDEIChair, ITU-T SG17 | E-mail : arnaud.taddei@broadcom.com |
| **Contact:** | Honey MAKOLACo-convenor, CG-COP | E-mail: HMakola@icasa.org.za  |
| **Contact:** | Elsayed ALICo-Convenor, CG-COP | E-mail: eali@cra.gov.qa  |

|  |  |
| --- | --- |
| **Abstract:** | This Liaison Statement informs Council Working Group on Child Online Protection (CWG-COP), ITU-D Q3/2, ITU-D Q6/1, ISO/IEC JTC 1 SC 27/WG 5 of the progress of the CG-COP as reported at the meeting of the ITU-T Study Group 17 (Geneva, 8 - 17 April 2025). |

ITU-T Study Group 17 informs you that the work of its Correspondence Group on Child online protection (CG-COP) has progressed well. The CG-COP has been working within SG17 with the aim to identify areas where current technical standards fall short in addressing emerging online threats to children as per the Terms of Reference (TOR) for the CG-COP.

SG17 shares the attached gap analysis for your information. The CG-COP will continue to function during the 2025–2028 study period. SG17 invites you to consider participation in the activities of the Correspondence Group through its mailing list: t25sg17cgcop@lists.itu.int. CG-COP is interested in pursuing more collaborative efforts in this regard.

ITU-T Study Group 17 will keep you informed of the progress of the Correspondence Group.

**Annex (Attachment): 1**

* Gap analysis on standards that support child online protection (COP) ([SG17-TD42/PLEN](https://www.itu.int/md/T25-SG17-250408-TD-PLEN-0042/en))

ANNEX

|  |  |  |
| --- | --- | --- |
| A black and white logo  AI-generated content may be incorrect. | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2025-2028 | **SG17-TD42/PLEN** |
| **STUDY GROUP 17** |
| **Original: English** |
| **Question(s):** | All/17 | Geneva, 8 – 17 April 2025 |
| **TD** |
| **Source:** | Co-convenors, CG-COP |
| **Title:** | CG-COP Output: Gap analysis on standards that support child online protection (COP) |
| **Contact:** | Honey MakolaIndependent Communications Authority of South AfricaSouth Africa | Tel: +27 71 643 2526E-mail: HMakola@icasa.org.za |
| **Contact:** | El-Sayed Ali Gomaa El-Sayed AliCommunications Regulatory AuthorityQatar | Tel: +974 4499 3649E-mail: eali@cra.gov.qa |

|  |  |
| --- | --- |
| **Abstract:** | This TD contains the output text from CG-COP on the gap analysis on standards that support child online protection (COP). |

**Introduction**

The ITU-T Study Group 17 (SG17) Correspondence Group on Child Online Protection (CG-COP) was formed to identify the scope and gaps in the Child Online Protection (COP) standardization within SG17 and other major standardisation bodies. This group conducted an in-depth review of current international standards, regulations and ongoing efforts related to protecting children online.

This report outlines the gaps identified in existing standards and provides a clear understanding of where further work may be needed. The analysis serves as a guide for SG17 to consider prioritising areas for new standards or enhancements to existing ones, helping to strengthen global efforts to protect children online. The findings may inform SG17's future work and ensure that standardization activities address emerging threats to child safety online.

**Keywords**

child online protection, gap analysis, standards

**CONTENTS**

|  **Page** |
| --- |
| [**1** **Scope 3**](#_Toc192501998)[**2** **References 3**](#_Toc192501999)[**3** **Terms and definitions 3**](#_Toc192502000)[3.1 Terms defined elsewhere 3](#_Toc192502001)[3.2 Terms defined here 4](#_Toc192502002)[**4** **Abbreviations 4**](#_Toc192502003)[**5** **Methodology 4**](#_Toc192502004)[**6** **Identification of risks / threats that children can face online 4**](#_Toc192502005)[**7** **Types of online harm experienced by children 5**](#_Toc192502006)[**8** **Security measures to address online threats and harm to children 6**](#_Toc192502007)[**9** **Existing gaps in standards to support child online protection 6**](#_Toc192502008)[9.1 Standardization gaps related to age assurance 6](#_Toc192502009)[9.2 Standardization gaps related to automated content moderation 8](#_Toc192502010)[**10** **Suggested ways forward for ITU-T Study Group 17 9**](#_Toc192502011)[10.1 Child age assurance 9](#_Toc192502012)[10.2 Automated content moderation 9](#_Toc192502013)[**Bibliography 10**](#_Toc192502014) |

**List of Tables**

|  **Page** |
| --- |
| [Table 1: COP GAP-01 6](#_Toc192501985)[Table 2: Gap analysis on age assurance standards 7](#_Toc192501986)[Table 3: COP-GAP-02 8](#_Toc192501987)[Table 4: Gap analysis on standards on automated content moderation 8](#_Toc192501988) |

**Gap analysis**

**Standards that support the Child Online Protection (COP) use case that may inform ITU-SG17**Draft version

**Scope**

The gap analysis for standards that support Child Online Protection (COP) within the mandate of ITU's SG17 aims to identify scope and gap for COP standardization in SG17 where current standards fall short in addressing emerging online threats to minors.

**References**

None.

**Terms and definitions**

**Terms defined elsewhere**

**3.1.1 age assurance** **[b-ISO/IEC DIS 27566-1]**: set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organizations to make *age-related eligibility decisions* (3.1.8) with varying *degrees of certainty* (3.3.4)

**3.1.2 child [b-CRC-1]:** every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier

**3.1.3 child sexual exploitation and abuse (CSEA) [b-ITU COP Guidelines]:** all forms of sexual exploitation and sexual abuse (CRC, 1989, art. 34), e.g. “(a) the inducement or coercion of a child to engage in any unlawful sexual activity; (b) The exploitative use of children in prostitution on or other unlawful sexual practices; (c) The exploitative use of children in pornographic performances and materials”

**3.1.4 content moderation [b-Roberts]:** the organized practice of screening user-generated content (UGC) posted to Internet sites, social media, and other online outlets, in order to determine the appropriateness of the content for a given site, locality, or jurisdiction

**3.1.5 cyberbullying, also referred as online bullying [b- ITU COP Guidelines]:** an intentional aggressive act carried out repeatedly by either a group or an individual using digital technology and targeting a victim who cannot easily defend themselves. It usually involves “using digital technology and the internet to post hurtful information about someone, purposely sharing private information, photos or videos in a hurtful way, sending threatening or insulting messages (via email, instant messaging, chat, texts), spreading rumours and false information about the victim or purposely excluding them from online communications. It may involve direct (such as chat or text messaging), semi-public (such as posting a harassing message on an e-mail list) or public communications (such as creating a website devoted to making fun of the victim).

**3.1.6 grooming / online grooming [b-Lux]:** the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person

**3.1.7 individual [b-ISO 29995]:** human being, i.e., a natural person, who acts as a distinct indivisible entity or is considered as such

**3.1.8 personal information [b-ITU COP Guidelines]:** individually identifiable information about a person, that is collected online. This includes the full name, contact details like home and email addresses, phone numbers, fingerprints or facial recognition material, insurance numbers or any other factor that permits the physical or online contacting or localization of a person. In this context it further refers to any information about a child and his or her entourage that is collected online by service providers online, including connected toys and the Internet of things and any other connected technology

**3.1.9 privacy [b-ITU-T X.800]:** the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
NOTE – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security

**3.1.10 sexting [b-ITU COP Guidelines]:** the sending, receiving, or exchanging of self-produced sexualized content including images, messages, or videos through mobile phones and/or the Internet

**3.1.11 user-to-user service (U2U) [b-OSA-UK]:** an internet service by means of which content that is generated directly on the service by a user of the service or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service

**Terms defined here**

None.

**Abbreviations**

|  |  |
| --- | --- |
| COP | Child Online Protection |
| CSEA | Child Sexual Exploitation and Abuse |
| CSAM | Child Sexual Abuse Material |
| E2EE | End-to-End Encryption |

**Methodology**

The gap analysis methodology is structured around assessing threats, vulnerabilities, and the resultant harms affecting minors during online interactions and what the applicable technical measures are in addressing such issues and to what extent those technical measures are standardized according to the mandate of the ITU-T SG17 and in other Standards Development Organizations.

The gap analysis follows a structured approach to identify gaps in current standards. The analysis consists of:

1. Assessing the potential risks that children may face online.
2. Identifying how these risks translate into actual harm.
3. Identifying potential security measures can be applied to address these threats and harms.
4. Identifying the gaps that exist in existing standards based on the identified security measures.
5. Suggesting proposed enhancements to existing frameworks and identifying areas requiring new standardization work.

This approach ensures an understanding of challenges and potential solutions, guiding the development of enhanced standards.

**Identification of risks / threats that children can face online**

The four categories (4 C's) framework below provides a structured approach to understanding the diverse risks children face in the digital environment. By categorizing these threats educators, parents, and policymakers can develop more effective strategies for safeguarding young internet users. The 4 C's are as follows:

1. **Content**: This category encompasses exposure to harmful material online, such as pornography, violence, hate speech, and misinformation. Children may inadvertently come across such content while browsing the internet or be deliberately targeted with harmful material.
2. **Contact**: Contact risks involve interactions with others on the internet that may lead to harm. This includes cyberbullying by peers, online harassment, grooming by predators, and any form of exploitation. The interactive nature of the internet, especially on social media platforms, chat rooms, and through instant messaging, increases the vulnerability of children to such risks.
3. **Conduct**: Conduct refers to children's own behavior online that may pose a risk to themselves or others. This includes engaging in cyberbullying, sharing personal or inappropriate content, and risky online behaviors such as sexting.
4. **Contract**: This relatively new category addresses the risks related to privacy and data protection, such as children unknowingly sharing personal information or being subjected to data collection practices by online services and applications. It also encompasses issues around digital consumerism, such as in-app purchases and exposure to targeted advertising.

**Types of online harm experienced by children**

Recognizing risks is different from harm. Where threats are potential sources of harm, vulnerabilities are weaknesses that threats can exploit, and harm is the negative impact from this exploitation. Below are some scenarios illustrating the variations:

* + **Risk**: A young person shares personal details (like location or school) on their profile, making them visible to strangers.
	+ **Harm**: Someone misuses that information to stalk or impersonate them, leading to distress or safety concerns.
	+ **Threat**: Online predators, cyberbullies, or scammers who exploit personal data or harass young users.

The [b- ITU COP Guidelines] identify several key harms that children may experience online. These harms arise from various online threats and are categorized as follows:

1. **Self-abuse and self-harm:** Exposure to content that encourages or depicts self-harm and suicidal behavior, or abuse can influence children to engage in such activities.
2. **Exposure to age-inappropriate content:** Children could be exposed to extremist, violent, or gory content, including online gambling. Such exposure can lead to desensitization to violence or engagement in high-risk behaviors. Harm can occur from isolated incidents of exposure or from cumulative exposure following repeated incidents or a single incident where a child is exposed to a combination of different harmful content.
3. **Radicalisation:** Online platforms can be used to manipulate children into adopting radical ideologies, hate speech, or extremist viewpoints which may lead to real-world consequences, including participation in / contributing to such activities
4. **Child sexual exploitation and abuse (CSEA):** This includes exposure to and involvement in activities such as the production and distribution of self-generated explicit content, sexual grooming by adults, viewing or being depicted in child sexual abuse material (CSAM), trafficking, and sexual exploitation in travel and tourism.
5. **Violation and misuse of personal data:** Harms in this category involve hacking, fraud, theft, (including identity theft), and other privacy breaches. It emphasizes the importance of protecting children's personal data as it can be collected, often without their knowledge or consent, and exploited for malicious purposes.
6. **Cyberbullying,** **Stalking, and** **Harassment:** Online hostility, including bullying, harassment, exclusion, and discrimination can have long-term emotional and psychological effects. Children may experience intimidation, threats or social isolation, both online and offline (as a result of their online activities).

**Security measures to address online threats and harm to children**

The following are potential technological measures to mitigate the threats and associated harm that may benefit from technical standardization work:

1. **Age assurance systems** for implementing age verification, age estimation and age inference mechanisms to prevent underage individuals from accessing adult-oriented content and platforms.
2. **Automated content moderation solutions** using perceptual hash matching technology in conjunction with Artificial intelligence (AI) models to support the detection and removal of illegal and harmful content, such as CSEA material. This measure aligns with the need for consistent, effective, and ethical practices in automated content moderation tools across platforms.
3. **Privacy-conscious content moderation solutions** that balance privacy concerns with the obligation to automatically detect and report illicit content, particularly for automatic content moderation in environments where end-to-end encryption (E2EE) is used. Such technical solutions could potentially increase child safety while maintaining user privacy in encrypted communications, addressing the challenges posed by E2EE on certain messaging platforms.

**Existing gaps in standards to support child online protection**

**Standardization gaps related to age assurance**

**Table 1: COP GAP-01**

|  |  |
| --- | --- |
| Gap identifier | COP GAP-01 |
| Title | Child age assurance standards |
| Tags | Age assurance, age verification, age inference, privacy, child safety, biometrics, child online protection, COP  |
| Ecosystem description | Online platforms, social media |
| Gap description | The current gap lies in the lack of immediately available, finalized global comprehensive technical standard for Age Assurance Systems, that are necessary for consistent and reliable implementation of age assurance. The table below illustrates this. |
| Future work | The process of developing standards has commenced however, no immediate standard is currently available for use. While standards are still under development, gaps remain, as outlined in the table below. To build upon existing standardization work, avoid duplication, and adapt to emerging standards for comprehensive child protection online, it is recommended to:* + **Monitor:** Track the development of ISO/IEC 27566 and consider collaboration to develop a common standard between ISO and ITU, and track the development of ETSI HF Technical Reports, Age Verification Pre-Standardization Study, IEEE.
	+ **Evaluate and adapt**: Upon completion of the ongoing standards, assess their effectiveness and determine if further standards development is needed.
 |
| Groups impacted | Online platforms, developers, policymakers, standardization entities  |

**Table 2: Gap analysis on age assurance standards**

| **SDO** | **Publication** | **Publication type** | **Description and applicability** | **Gap analysis** |
| --- | --- | --- | --- | --- |
| ISO | [b-ISO/IEC DIS 27566-1][b-ISO/IEC WD 27566-3.2] | Standard | ISO has work ongoing on the ISO/IEC 27566 Standard for age assurance systems under ISO/IEC JTC 1/SC 27. This Standard is broken down into two documents: Part 1: Framework [b-ISO/IEC DIS 27566-1]; ISO/IEC 27566-2- Part 2: Technical approaches and guidelines for use, and Part 3: Benchmarks for Benchmarking Analysis [b-ISO/IEC WD 27566-3.2].Part 1 [b-ISO/IEC DIS 27566-1] is a global framework level document: all age assurance systems worldwide will be built around this standard, which is a framework for gaining age assurance for age related eligibility decisions.  | The ISO/IEC 27566 is a Standard for Age Assurance Systems, which includes a comprehensive framework and technical guidelines. However, its work is still under development, and it will not be published until at least Spring 2025, so its final content is still unknown which is the gap. There is also potential cost barriers associated with accessing draft standards for comments. |
| IEEE | [b-IEEE 2089.1] | Standard | This standard establishes a framework for the design, specification, evaluation, and deployment of age verification systems. | However, it indicates the requirements for establishing different levels of confidence (asserted, standard, enhanced, and strict) associated with the types of age assurance systems and requirements for privacy protection, data security, and information systems management that are specific to the age assurance process. It does not specify detailed information about countermeasures (i.e., anti-spoofing techniques), methods to detect presentation attacks, algorithms, or sensors and Methods to assess the overall system-level security or vulnerability. |
| ITU | [b-ITU FGMV-12] | Technical Report | This document describes age verification methods in the metaverse to protect children from online threats, emphasizing compliance with regulations like GDPR and minimal data use. It advocates for risk assessment frameworks and trusted third-party verification for privacy and interoperability. | This technical report just focuses on metaverse platforms, so there is a need for broader applicability across various digital environments and consistent implementation of age assurance methods for children to ensure child online protection. While also balancing security with minimal data collection remains a challenge. |
| ETSI | [b-ETSI-DTR/HF-00301567][b-ETSI-DTR/HF-00301568] | Technical Report*(draft)* | ETSI are currently working on Technical Reports focused on Human Factors (HF); Age verification pre-standardization study; Part 1: Stakeholder requirements which aims to establish and analyse stakeholder requirements for age verification, laying the groundwork for future European standards in this field, as requested in the Digital Services Act and Part 2: Solution and standards landscape which seeks to identify the existing solutions and standards landscape for age verification, and how they can be used to meet the stakeholder requirements for age verification as identified in Part 1. | The work remains in progress and standards/technical reports are not yet fully ready. |

**Standardization gaps related to automated content moderation**

**Table 3: COP-GAP-02**

|  |  |
| --- | --- |
| Gap identifier | COP GAP-02 |
| Title | Automated content moderation |
| Tags | Child safety, AI, content moderation, harmful content, self-harm |
| Ecosystem description | Online platforms, social media, child-focused apps |
| Gap description | Lack of global technical standards specifically addressing expected performance of automated content moderation technology for harmful content targeting children. This gap is particularly pronounced in the context of user-generated content within user-to-user (U2U) services.Further, while there is an increasing adoption of end-to-end encryption by large social media platforms, service providers are technically unable to use content moderation tools to detect harmful content for children in direct messaging within an end-to-end encryption environment which creates a standardization gap. |
| Future work | Perceptual hash matching technology is widely used in content moderation to identify and remove illegal content, as well as to combat misinformation and prevent the spread of harmful content online. However, there is currently no unified, comprehensive technical standard specifically for perceptual hash matching technology in automated content moderation. Developing such a technical standard could ensure consistency and effectiveness across platforms. Its deployment should reflect ethical practices.SG17 could consider technical solutions and as needed, call for contribution for addressing the gap of end-to-end encryption.  |
| Groups impacted | Developers, content providers/social media platforms, standardization entities  |

**Table 4: Gap analysis on standards on automated content moderation**

| **SDO** | **Publication** | **Publication type** | **Description and applicability** | **Gap analysis** |
| --- | --- | --- | --- | --- |
| ISO | [b-ISO/IEC 10118-3] | Standard | A standard that specifies different cryptographic hash functions, which are fundamental to the operation of hash matching technology.This document specifies dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this document are based on the iterative use of a round-function. Distinct round-functions are specified, giving rise to distinct dedicated hash-functions. | While [b-ISO/IEC 10118-3] provides a solid foundation for the secure creation of hash functions, it doesn’t address the specific application of hash matching technology in automated content moderation. To fully address the needs of content moderation, especially for protecting children online, additional technical standards or guidelines are required to cover automated content moderation application-specific guidance, integration with other technologies and performance benchmarks. |

**Suggested ways forward for ITU-T Study Group 17**

ITU-T Study Group 17 may be able to address the identified gaps in child online protection standards in collaboration with other SDOs, promoting a safer and more secure digital environment for children worldwide through the following ways.

**Child age assurance**

Although some standards have been developed, gaps persist, and other standards’ development are still ongoing. To build on existing work, avoid the risk of effort duplication, leverage on existing work and align with emerging standards for comprehensive child protection online, the following actions are recommended:

1. SG17 to collaborate with relevant SDOs and regulatory bodies (as identified above) to ensure that the developed standards are globally applicable and do not conflict with existing standards, in the following areas:
	1. ISO/IEC 27566,
	2. ETSI HF Technical Reports on the Age Verification Pre-Standardization Study
	3. IEEE initiatives, and

This collaboration could be through joint working groups to ensure consistency and avoid duplication of efforts.

1. It is recommended that Q10/17 prioritize identified work in the gap analysis and integrate into the study items, given the urgent need to address emerging challenges effectively.
2. Evaluate and adapt: Once ongoing standards are completed, assess their effectiveness and determine if additional standards development is necessary to fill any remaining gaps.

**Automated content moderation**

Given the findings of the gap analysis, CG-COP has identified potential technological measures for automated content moderation which could significantly enhance the ability of member states to protect children online, while respecting their sovereignty. To that end, SG17 could, in the interim, study automated content management in the format of technical reports in collaboration with relevant SDOs and other bodies:

1. To develop a unified standard for hash matching technology for the automated content moderation application. Perceptual hash matching technology is essential for content moderation, particularly in identifying and removing illegal content and different categories of child harmful content. However, the lack of a unified, comprehensive technical standard for this technology presents a gap. Developing such a standard could help ensure consistency and effectiveness of this technology, applied across platforms. Its deployment should reflect ethical practices.
2. To consider technical solutions and as needed call for contribution for addressing the detection of harmful content aimed at children within end-to-end encrypted U2U services.

**Bibliography**

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*

[b-ITU COP Guidelines] ITU Guidelines for policy-makes on Child Online Protection (2020),
https://www.itu-cop-guidelines.com/\_files/ugd/24bbaa\_b5fec426d50d4a21b721489099b5781f.pdf

[b-ITU FGMV-12] Technical Report ITU FGMV-12 (2023), *Children's age verification in the metaverse*

[b-CRC-1] United Nations Convention on the Rights of the Child Article 1- Entry into force: 2 September 1990.

[b-ETSI-DTR/HF-00301567] ETSI Draft Technical Report, *Age Verification Pre-Standardization Study Part 1: Stakeholder Requirements*

[b-ETSI-DTR/HF-00301568] ETSI Draft Technical Report, *Age Verification Pre-Standardization Study Part 2: Solutions and Standards Landscape*

[b-IEEE 2089.1] IEEE 2089.1 (2024), *IEEE Standard for Online Age Verification*

[b-ISO 29995] ISO 29995 (2021), *Education and learning services — Vocabulary*

[b-ISO/IEC 10118-3] ISO/IEC 10118-3 (2018), *IT Security techniques — Hash-functions Part 3: Dedicated hash-functions*

[b-ISO/IEC DIS 27566-1]ISO/IEC DIS 27566-1, *Information Security, cybersecurity and privacy protection – Age Assurance Systems Part 1: Framework*

[b-ISO/IEC WD 27566-3.2]ISO/IEC DIS 27566-1 WD 27566-3.2, *Information Security, cybersecurity and privacy protection – Age Assurance Systems Part 3: Benchmarks for benchmarking analysis*

[b-Lux] Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (2016)
https://ecpat.org/luxembourg-guidelines/

[b-OSA-UK] Online Safety Act 2023, Chapter 50

[b-Roberts] Roberts, S.T. (2017), *Content Moderation*. Schintler, L., McNeely, C. (eds) Encyclopedia of Big Data. Springer, Cham.
https://doi.org/10.1007/978-3-319-32001-4\_44-1

|  |  |
| --- | --- |
| [b- ISO/IEC 2382] | ISO/IEC 2382:2015(en) Information Technology-Vocabulary. |
| [b- International Humanitarian Law Databases]  | Article 34-Convention on the Rights of the Child, 20 November 1989. |
| [b- Ofcom-UK] | Protecting children from harms online - Volume 5: What should services do to mitigate the risks of online harms to children? |
| [b- Ofcom-UK] | Protection of Children Code of Practice for user-to-user services. |
| [b- Ofcom-UK] | Protecting children from harms online - A summary of consultation |
| [b- Internet Watch Foundation -IWF] | ICO call for views -Data protection and content moderation. |
| [b- Ofcom-UK] | Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services-Annex 2. |
| [b-ISO/IEC 24760-1:2019] | IT Security and Privacy - A framework for identity management. Part 1: Terminology and concepts |
| [b-T20 (Think 20) Brazil 2024 Task Force 05] | Designing Digital Global Governance with children’s best interests and their rights as a priority  |
| [b-CEN and CENELEC WORKSHOP AGREEMENT] | Age-appropriate digital services framework - CWA 18016. |

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