Final Communiqué

Global Age Assurance Standards Summit

The Global Age Assurance Standards Summit, convened in Manchester, United Kingdom between 14 and 16 April 2026, brought together governments, regulators, international organisations, civil society, academia, industry leaders, age assurance service providers, standards developers and technical experts to reflect the position, state of the art and development of age assurance as of April 2026.

This Communique represents a consensus snapshot of the state of play in age assurance practice, policy and standardisation. It is intended as a benchmark in the continuing evolution of age assurance globally.

Headline

Age Assurance Has Come of Age

International standards have been published.
Regulatory frameworks are operational.
Enforcement is underway.

The global conversation has entered a new phase. It has moved from whether age assurance can be done, to how it must be implemented — lawfully, proportionately and with respect for fundamental rights.

Definition

Age assurance is a 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 with varying degrees of certainty [ISO/IEC 27566-1: 2025]

Preamble

Recognising that since the inaugural Global Age Assurance Standards Summit in Manchester in 2024, and the consolidation of consensus in Amsterdam in 2025, age assurance has moved from proof of concept to operational deployment across multiple jurisdictions;

Recalling that the 2024 Communiqué affirmed that *"Age Assurance can be done"* and that the 2025 Communiqué confirmed that it can be deployed proportionately, effectively and in a privacy-preserving manner;

Welcoming the publication of **ISO/IEC 27566-1 – Age Assurance Systems – Part 1: Framework**, which for the first time establishes an internationally agreed, rights-respecting and risk-based framework for age assurance systems;

Recognising that the publication of ISO/IEC 27566-1 represents a major milestone in the maturation of the age assurance ecosystem by:

- Establishing common terminology;
- Distinguishing clearly between age verification, age estimation and age inference under the wider taxonomy of age assurance;
- Describing assurance levels and confidence;
- Supporting structured, risk-based implementation;
- Providing a reference model for regulators, platforms and providers;

Noting the continuing development of ISO/IEC 27566-2 and ISO/IEC 27566-3, and welcoming the publication of **IEEE 2089.1-2024**, reflecting growing alignment between international standards bodies, certification schemes and regulatory authorities;

Recognising that the existence of internationally recognised standards now enables:

- Greater comparability between systems;
- Clearer procurement and compliance decisions;

- More consistent regulatory guidance;
- A foundation for certification, audit and mutual recognition frameworks;

Affirming that these standards do not prescribe a single technical solution, but instead provide a structured, interoperable and technology-neutral framework for proportionate decision-making;

Recognising that regulatory regimes and emerging global frameworks have entered into force or implementation phases requiring demonstrable, proportionate and effective age assurance measures;

Observing that enforcement authorities across jurisdictions are now imposing significant sanctions and compliance measures where platforms fail to implement appropriate protections for children online, marking a transition from policy debate to regulatory enforcement;

Recalling that the **UN Committee on the Rights of the Child**, in General Comment No. 25 (2021), affirmed that children's rights apply fully in the digital environment, and that States must ensure that businesses respect those rights;

Reaffirming that age assurance must be deployed that are consistent with the principles of necessity, proportionality, transparency, accountability and non-discrimination, respecting the privacy, data protection rights of both children and adults;

Recognising that age assurance is not a single technology but a structured decision-making process, adaptable to context and risk, supported by privacy-enhancing technologies, secure architectures and interoperable standards;

Acknowledging the growing technical challenges presented by synthetic media, generative AI systems and increasingly sophisticated evasion techniques, and the need for standards and certification mechanisms to remain responsive to technological development;

Recognising further that adults, as well as children, are subject to age-related eligibility decisions, and that the protection of children must not come at the expense of lawful adult access to goods and services, neither should it unreasonably or disproportionately limit lawful forms of expression between adults;

Affirming that international standards, certification mechanisms and mutual recognition frameworks can reduce fragmentation, support innovation, enhance trust and provide legal certainty for regulators, platforms and service providers;

Concluding that age assurance has entered a phase of global implementation in which standards, regulation, certification and enforcement must operate coherently to protect children's rights while preserving privacy, proportionality and trust in the digital environment.

Call to Action

Bearing in mind the principles of necessity, proportionality, transparency, accountability and non-discrimination, as well as the evolving capacities of the child, the Communique identifies the following priorities:

1. Align Enforcement with Standards

Regulators should reference internationally recognised standards, including ISO/IEC 27566-1, in guidance and enforcement activity to promote clarity, reduce fragmentation and enable consistent, auditable compliance across jurisdictions.

2. Move from Deployment to Demonstrable Assurance

Organisations implementing age assurance should be able to demonstrate:

- Why age assurance is required,
- What level of assurance is proportionate,
- How the chosen method aligns with recognised standards,
- How fundamental rights risks have been mitigated.

3. Protect Children Without Creating Surveillance

Age assurance must not become:

- A mechanism for revealing identity,
- A tool for persistent tracking or cross-service correlation of user activity,
- A gateway to disproportionate data collection,
- A system to exclude children or adults from the digital environment.

Architectures should require privacy-preserving, attribute-based and data-minimising approaches wherever feasible.

4. Embed Human Rights Impact Assessments

Age assurance systems should be accompanied by documented, reviewable and periodically updated assessments addressing:

- Privacy,
- Data protection,
- Equality and non-discrimination,
- Accessibility,
- The user experience, particularly for children.

5. Address Global Interoperability

Stakeholders should work toward:

- Mutual recognition of age attributes,
- Interoperable credentials,
- Avoiding conflicting technical mandates.
- Mechanisms that minimise the need for repeated verification across services while preventing unintended cross-service tracking.

6. Support Inclusion

Special attention must be paid to:

- Individuals without formal identity documentation or who are not literate,
- Users in low-connectivity environments,
- Shared device contexts,
- Persons with a limited capacity to understand or navigate age assurance processes.

Guiding Principles

The Global Age Assurance Standards Summit reaffirms the foundational principles articulated in 2024 and 2025 and consolidates them into six operational pillars reflecting the realities of 2026: standardisation, deployment at scale and active enforcement.

These principles are intended to guide regulators, policymakers, service providers, technology developers and conformity assessment bodies.

Principle 1: Human Rights and the Best Interests of the Child

Age assurance systems must be grounded in international human rights law and must respect the rights to privacy, data protection, access to age-appropriate information, non-discrimination and protection from harm. These rights must be safeguarded not only as a matter of policy intent, but through the design, development and operation of age assurance systems. Age assurance must serve the best interests of the child while also respecting the rights and freedoms of adults.

Guideline 1.1
Implementation should balance protection and provision. Measures designed to protect children from harm should not restrict their access to age-appropriate content, products or services, nor impose unjustifiable limitations on lawful adult access, unless such restrictions are necessary, proportionate and evidence-based.

Guideline 1.2
Systems should take account of the evolving capacities of children and the diversity of user circumstances, ensuring that age-related eligibility decisions are context sensitive and comply with relevant local regulations.

Guideline 1.3
Age assurance must enhance rights, not erode them. Any deployment should demonstrably strengthen the protection of children's rights through its design and implementation, without disproportionately or unreasonably impacting or limiting the rights of adults.

Principle 2: Risk-Based and Proportionate Implementation

Age assurance is not a one-size-fits-all solution. Its implementation must be based on a documented, reasoned and reviewable assessment of risk which cannot be meaningfully mitigated by less intrusive measures. Such assessments should be capable of demonstrating, where appropriate, transparency and external scrutiny.

Guideline 2.1
Organisations should conduct and maintain a documented risk assessment that evaluates the nature and severity of potential harm, the likelihood of exposure, the vulnerability of the user group, the functionality of the service, and the relevant jurisdictional regulatory environment before determining the level of assurance required.

Guideline 2.2
The level of assurance deployed should correspond to the level of risk identified. Lower-risk environments may justify lighter-touch methods, whereas higher-risk contexts may require stronger and more reliable assurance mechanisms.

Guideline 2.3
Proportionality requires clear reasoning, evidence-based decision-making and periodic reassessment. Risk assessments and resulting implementation decisions should be kept under review and updated as technologies, risks, regulatory expectations and patterns of use evolve.

Principle 3: Privacy and Data Minimisation by Design

Age assurance systems must be purposefully designed to protect privacy as a foundational requirement.

Guideline 3.1
Systems should confirm an age or age-range without revealing or allowing the discovery of identity, minimise the collection of personal data, and avoid retaining personal data beyond what is strictly necessary for the purpose of making an age-related eligibility decision.

Guideline 3.2
Hard identifiers, such as passports or biometric data, should not be stored, reused or

aggregated across services, nor used in ways that enable correlation or linkability of user activity across different services or contexts, unless this is demonstrably necessary and proportionate.

Guideline 3.3
Privacy-enhancing approaches — including attribute-based credentials, zero-knowledge mechanisms and decentralised models — should be preferred by default where they can meet the relevant assurance need. Age assurance must not become a gateway to identity surveillance or function creep.

Principle 4: Standards-Based Interoperability and Technical Integrity

With the publication of IEEE 2089.1, ISO/IEC 27566-1 and related standards, age assurance now benefits from a shared international framework that supports clarity and comparability.

Guideline 4.1
Implementation should use standardised terminology, clearly define the type of assurance provided, and communicate levels of confidence and uncertainty in a consistent and intelligible manner.

Guideline 4.2
Regulators are encouraged to reference internationally recognised standards in guidance and enforcement to reduce fragmentation, promote cross-border coherence and provide legal certainty.

Guideline 4.3
Interoperability should be pursued to avoid unnecessary duplication of checks across services and to support secure, reusable and user-friendly assurance mechanisms.

Principle 5: Digital Inclusion and Accessibility

Age assurance must not exclude legitimate users or create new forms of digital inequality.

Guideline 5.1
Systems should account for individuals without formal identity documentation, users in shared device environments, persons in low-connectivity regions, persons with disabilities, those facing socioeconomic barriers or persons facing any other barriers to inclusion.

Guideline 5.2
Where possible, multiple pathways to demonstrate age eligibility should be made available to accommodate diverse circumstances and capabilities. It should also be assessed how these pathways operate in practice and whether they disproportionately exclude or burden certain groups.

Guideline 5.3
Inclusion is essential to legitimacy and fairness. Systems which are unnecessarily burdensome risk excluding too many people thereby creating risks which undermine trust.

Principle 6: Transparency, Accountability and Independent Assurance

In an era of active enforcement and significant financial penalties for non-compliance, coupled with a dynamic and competitive marketplace of providers, transparency and accountability are essential components of lawful and trustworthy age assurance.

Guideline 6.1
Organisations deploying age assurance should be able to demonstrate the rationale for implementation, the proportionality of the chosen method, alignment with recognised standards, the results of risk and impact assessments and the accuracy and performance characteristics of the system. Systems should be capable of being tested and evaluated, including with respect to measures taken to identify and address bias and discrimination.

Guideline 6.2
Independent certification, audit and conformity assessment mechanisms enhance trust, strengthen accountability and provide clarity for regulators, service providers and users. Such mechanisms should enable effective scrutiny of system design, performance and governance.

Guideline 6.3
In clear and accessible language users should be informed why age assurance is required, what data are being processed, for how long it will be retained, and what rights and remedies are available to them. Users should have access to appropriate mechanisms to question or challenge a result and seek a correction if they believe it is inaccurate or unfair.