

IEEE Standard for Online Age Verification

IEEE Consumer Technology Society

Developed by the
Emerging Technology Standards Committee

IEEE Std 2089.1™-2024

IEEE Standard for Online Age Verification

Developed by the

Emerging Technology Standards Committee
of the
IEEE Consumer Technology Society

Approved 21 March 2024

IEEE SA Standards Board

Abstract: Framework for the design, specification, evaluation, and deployment of online age verification systems are established in this standard. This standard is the second in a family of standards focused on the 5Rights principles.

Keywords: age, age assurance systems, child, children, children's rights, IEEE 2089™, IEEE 2089.1™

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 24 May 2024. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-0796-0 STD26980
Print: ISBN 979-8-8557-0797-7 STDPD26980

*IEEE prohibits discrimination, harassment, and bullying.
For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all IEEE standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers involved in technical working groups are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and shall not be considered or inferred to be, the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE or IEEE SA. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter’s views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments or questions, except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory

¹Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

²Available at: <https://standards.ieee.org/about/contact/>.

requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional

³Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴Available at: <https://standards.ieee.org/standard/index.html>.

Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, data privacy, and interference protection practices and all applicable laws and regulations.

⁵Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this IEEE standard was completed, the IEEE P2089.1 Working Group had the following membership:

Iain Corby, Chair
Julie Dawson, Vice Chair

Tony Allen
Michael Bolcerek
Becky Burgess
Christian Czeskleba
Matt Eastwood

Kostas Flokos
Alastair Graham
Duncan McCann
Lee McElhinney
Andrew O'Brien

Omari Rodney
Julian Sargeson
Denise Tayloe
Onur Yürüten
Alex Zeig

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Azfar Adib
Mila Aliana
Boon Chong Ang
Max Carlson

Iain Corby
Werner Hoelzl
Ruth Lewis
Rajesh Murthy

Bansi Patel
Cam Posani
Jhony Sembiring
Walter Struppler

When the IEEE SA Standards Board approved this standard on 21 March 2024, it had the following membership:

David J. Law, Chair
Jon W. Rosdahl, Vice Chair
Gary Hoffman, Past Chair
Alpesh Shah, Secretary

Sara R. Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W. Hotchkiss
Hao Hu

Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano

Paul Nikolich
Robby Robson
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2089.1-2024 IEEE Standard for Online Age Verification .

This standard is part of the family of IEEE 2089 standards that seek to design the digital world with children in mind. Each of these standards is underpinned by the assertion that children should have access to the digital world for their benefit and the benefit of society more broadly. If that is the case, then it follows that the digital world should be designed to account for their age, development capacity, and rights. Children’s established rights are set out in the convention on the rights of the child and interpreted in GC 25 (2021) the relevance of children’s right to the digital environment. In the context of age assurance, the right to access the digital world is considered, and therefore, age assurance should be proportional to risk, systems should encourage use by being easy to use, and they respect children’s right to privacy, protection from harm (commercial, physical, emotional), and their right to participate. Above all, those that use the standard should follow the overarching principle that where business interests come into conflict with the needs of children, the best interest of the child is paramount.

The IEEE 2089 family of standards are used by businesses and organizations that are committed to building the digital world children deserve.

No standard can provide unconditional consistency with all laws and regulations. Users of this standard are responsible for referring to and observing all applicable legal and regulatory requirements, and should refer questions of compliance to competent legal counsel with expertise in the relevant jurisdiction.

Contents

1. Overview	11
1.1 Scope	11
1.2 Purpose	11
1.3 Word usage	12
1.4 Use of the standard	12
1.5 Process overview	13
2. Normative references	14
3. Definitions, acronyms, and abbreviations	15
3.1 Definitions	15
4. Acronyms and abbreviations	21
5. Conformance	21
6. Key concepts and application	22
6.1 General application	22
6.2 Specified context of use	23
6.3 The organization	23
6.4 Stakeholders	24
6.5 Stages and processes	26
7. Roles and responsibilities of key actors in the age assurance process	26
7.1 General	26
7.2 Role descriptions	26
7.3 User	28
8. Determining the need for age assurance (“determination phase”)	28
8.1 Purpose	28
8.2 Outcomes	28
8.3 Activities and tasks	29
8.4 Inputs	30
8.5 Outputs	30
9. Selecting the method(s) of age assurance (“selection phase”)	30
9.1 Purpose	30
9.2 Outcomes	30
9.3 Activities and tasks	31
9.4 Inputs	32
9.5 Outputs	33
10. Assuring the age of a user (“assurance phase”)	33
10.1 Purpose	33
10.2 Outcomes	33
10.3 Activities and tasks	33
10.4 Inputs	34
10.5 Outputs	35
11. Categorizing the level of confidence with which the assurance has been completed (“categorization phase”)	35
11.1 Purpose	35
11.2 Outcomes	35
11.3 Activities and tasks	35

11.4	Inputs	36
11.5	Outputs	36
12.	Exchanging the results of age assurance checks with other organizations (“interoperability phase”)	36
12.1	Purpose	36
12.2	Outcomes.....	36
12.3	Activities and tasks	36
12.4	Inputs.....	37
12.5	Outputs	37
13.	Protecting the privacy of users when undertaking age assurance (“privacy phase”)	37
13.1	Purpose	37
13.2	Outcomes.....	38
13.3	Activities and tasks	38
13.4	Inputs.....	38
13.5	Outputs	38
14.	Securing data relating to users used when undertaking age assurance (“data security phase”).....	39
14.1	Purpose	39
14.2	Outcomes.....	39
14.3	Activities and tasks	39
14.4	Inputs.....	39
14.5	Outputs	39
Annex A (normative)	Five standard levels of age assurance derived from six indicators of confidence in age assurance output	40
Annex B (normative)	Assessing the risk to children: The 4 Cs of online risk	47
Annex C (informative)	Bibliography	53

IEEE Standard for Online Age Verification

1. Overview

1.1 Scope

This standard establishes a framework for the design, specification, evaluation, and deployment of age verification systems. The term ‘age assurance’ includes ‘age verification’ and ‘age estimation’ methods unless otherwise stated, and where consistent with all applicable laws and regulations. It includes the following:

- The key terms, definitions, and abbreviations, together with the roles and responsibilities of key actors in the age assurance process.
- Requirements for establishing different levels of confidence (asserted, standard, enhanced, and strict) associated with the types of age assurance systems.
- 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.
- Methods to assess the overall system-level security or vulnerability.

1.2 Purpose

This standard provides a set of processes for digital services to verify or estimate the age or age range of a user, to a proportionate degree of accuracy and certainty, when determining the age of a child to allow organizations to enable access to their products and services to suitable age-groups, with the rights and needs of children in mind. This is essential to creating a digital environment that supports, by design and delivery, children’s safety, privacy, autonomy, agency, and health, specifically providing a set of guidelines and best practices and thereby offering a level of validation for age assurance decisions that may be either required by law or voluntarily implemented for business or social reasons.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{6,7}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

1.4 Use of the standard

The standard describes the set of processes by which leaders, managers, engineers, and technologists can undertake online age assurance.

In addition, any age assurance system should, as a minimum, provide the following:

- a) Protects the privacy of users in accordance with applicable laws, including the data protection laws and obligations under the treaties set out at list item k).
- b) Is proportionate having regard to the risks arising from the product or service and to the purpose of the age assurance system.
- c) Offers functionality appropriate to the capacity and age of a child who might use the service.
- d) Is secure, shall not expose users or their data to unauthorized disclosure or security breaches, and shall not use data gathered for the purposes of the age assurance system for any other purpose.
- e) Provides appropriate mechanisms and remedies for users to challenge or change decisions if their age is wrongly identified.
- f) Is accessible and inclusive to users with protected characteristics.
- g) Does not unduly restrict access of children to services to which they should reasonably have access, for example, news, health, and education services.
- h) Provides sufficient and meaningful information for a user to understand its operation, in a format and language that they can be reasonably expected to understand, including if they are a child.
- i) Is effective in verifying or estimating the age or age range of a user, to a proportionate degree of accuracy and certainty to allow organizations to enable access to their services to suitable age-groups, with the rights and needs of children in mind.
- j) Does not rely solely on users to provide accurate information.
- k) Is compatible with applicable data protection legislation and the United Nations Convention on the Rights of the Child and General Comment No. 25 (2021) on children's rights in relation to the digital environment.

⁶The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁷The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

No standard can provide unconditional consistency with all laws and regulations, and compliance with this standard does not constitute compliance with applicable legal and regulatory requirements. Users of this standard are responsible for referring to and observing all applicable laws and regulations, and should refer questions of compliance to competent legal counsel with expertise in the relevant jurisdiction.

It provides implementable processes to help align innovation with securing age-appropriate design for software engineering and system design and, in doing so, reduces risk and, wherever possible, amplifies the benefits of the digital world for end users who are considered children according to applicable laws and regulations.

The standard sits on the values of 5Rights Foundation’s principles and reflects the rights of children under the United Nations Convention on the Rights of the Child, including their right to participate in the digital world. Many digital systems impact children in intended or unintended ways and, therefore, should take them into account. All organizations for which that is the case are encouraged to use this standard to help make that engagement age appropriate. This standard is based on the foundation that the ‘best interests’ of the child are placed in primary focus during the design of digital services.

To reach this goal, this standard supports organizations in ascertaining whether age assurance is required, and if so, how best to implement it. It is applicable within any life cycle model or set of methods for systems and software engineering and/or new or modified product or service development including brokering children’s data. If organizations have existing systems that cause risks to children, then the processes in this standard can be used for reiteration of analysis and redress.

Data privacy and security are complex and highly regulated areas of law, particularly as related to children and young people. The relevant legal definitions and requirements are rapidly evolving, and may vary at the local, state, national, and regional level.

1.5 Process overview

The goal of this standard is to allow organizations to enable access to their services to suitable age-groups, with the rights and needs of children in mind. Age appropriateness includes a variety of values that support children. For example, values such as sustainability, privacy, usability, convenience, controllability, accountability, inclusivity, evolving capacity, and children’s rights can be promoted by using this standard. This standard also supports values or attributes in systems typically considered in system engineering, such as functionality, efficiency, and effectiveness. An overview of the key processes in this standard is depicted in [Figure 1](#).

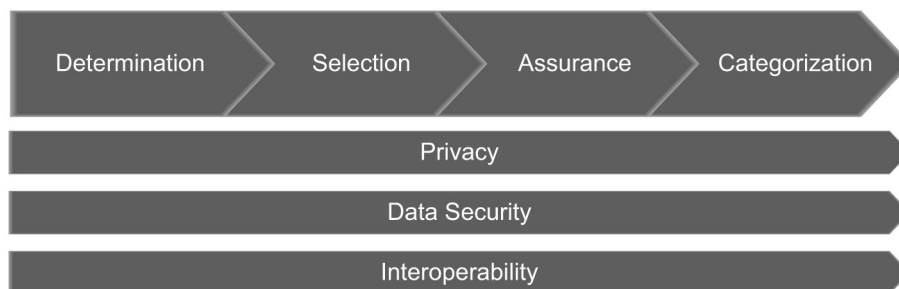


Figure 1—Phases for age assurance

The first four processes run sequentially as follows:

- a) Determination—undertake an initial overview of a service or product and identify the statutory, regulatory, contractual, and ethical requirements for age assurance.

- b) Selection—select the most appropriate method or methods of age assurance that meet the standards for age assurance.
- c) Assurance—undertake assurance of the age or age range of each user.
- d) Categorization—categorize the level of confidence to which the assurance has been completed.

The remaining three processes underpin the first four, and should be applied continuously:

- e) Privacy—ensure age assurance solutions protect the privacy of users by design.
- f) Data security—ensure that any personal data used during age assurance or retained after an age assurance has been completed is stored securely.
- g) Interoperability—allow an age assurance provider to exchange the results of an age assurance process with another age assurance provider in a privacy preserving fashion.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 2089TM, IEEE Standard for an Age-Appropriate Digital Services Framework Based on the 5Rights Principles for Children.^{8,9}

ISO 9000:2015, Quality management systems—Fundamentals and vocabulary.¹⁰

ISO Guide 73:2009 (withdrawn), Risk management—Vocabulary.

ISO/IEC 25010:2011, Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models.

ISO/IEC/IEEE 15288:2015, Systems and software engineering—System life cycle processes.

ISO/IEC/IEEE 29148:2018, Systems and software engineering—Life cycle processes—Requirements engineering.

United Nations Committee on the Rights of the Child General Comment (25), 2021 on Children’s Rights in Relation to the Digital Environment.

United Nations Convention on the Rights of the Child (UNCRC), 1989.

United Nations Resolution Promotion and Protection of the Rights of Children (78th Session, 2023).

⁸The IEEE standards or products referred to in this clause are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

⁹IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>).

¹⁰ISO publications are available from the International Organization for Standardization (<https://www.iso.org/>) and the American National Standards Institute (<https://www.ansi.org/>).

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.¹¹

accuracy: The degree of agreement between the observed value and the conventionally true value of the quantity being measured.

activity: A set of cohesive and purposeful tasks of a process.

age appropriate: Something that is suitable or appropriate for a person of a particular age.

NOTE 1—This concept is often, but not exclusively used in relation to children—a demographic who develop rapidly over a short space of time.¹²

NOTE 2—In the digital context, the concept of age appropriate is most associated with the Age-Appropriate Design Codes applicable in the UK and the state of California that set out data protection measures to benefit children.

age assurance: An umbrella term for both age verification and age estimation solutions. The word “assurance” refers to the varying levels of certainty that different solutions offer in establishing an age or age range.

NOTE—Age assurance may provide a specified level of confidence, but cannot guarantee accuracy in all cases.

age assurance provider: A company that supplies age verification or age estimation technology or services to a relying party.

age estimation: Any process that establishes a user is likely to be of a certain age, fall within an age range, or is over or under a certain age.

age estimation provider: A company that supplies age estimation technology or services to a relying party.

NOTE—Age estimation methods include, but are not limited to, artificial intelligence-based facial or voiceprint age analysis, and automated analysis of behavioral and environmental data, such as comparing the way a user interacts with a device with other users of the same age and metrics derived from motion analysis, or by testing their capacity or knowledge.

age verification (“AV”): A system that relies on hard (physical) identifiers and/or verified sources of identification that provide a high degree of certainty in determining the age of a user based on a specific date of birth. They include, but are limited to, hard identifiers (passports or other ID), managed databases both commercial or publicly held, as well as authoritative third parties, such as parents and carers.

age verification provider: A company that supplies age verification technology or services to a relying party.

age verification practice statement: A document that records the outputs of the processes in IEEE Std 2089.1™ used for the purposes of certification. It should comprise, at a minimum, four parts (part 1—determination; part 2—methods; part 3—child data practice impact assessment; part 4—data security certification).

assurance: The word “assurance” refers to the varying levels of certainty that different solutions offer in establishing an age or age range.

¹¹*IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

¹²Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

audit: See ISO/IEC/IEEE15288: 2015.¹³

NOTE—The scope includes professional and industry codes of practice.

authentication: A process to verify that someone is who they claim to be when they try to access a computer or online service.

balancing: Where one right comes into conflict with another, they should be balanced so that the “best interests” of the child is paramount.

best interest: Refer to UNCRC General Comment No. 14, Para.4 and General Comment No. 5, Para. 12.

benefit: A positive outcome that is voluntarily or involuntarily created by an act, system, or process.

binding: The process of connecting evidence of age with an individual person to whom it refers or to a particular device.

biometrics: The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns).

biometric: A measurement derived from physical characteristics, such as fingerprints, DNA, or retinal patterns, for use in verifying the identity of individuals or estimating their age.

NOTE—Biometric data is not always personally identifiable information as it may be insufficient to identify uniquely any individual, as is the case when it is used for the purposes of age estimation.

buffer: The period of time between the age at which a restriction is required, and the age that is tested using age estimation, to give a specified level of confidence in test.

certainty: The state of having no doubt or knowing exactly that something is true, or known to be true, correct, exact, or effective.

certification: The provision by an independent body of written assurance (a certificate) that the product, service, or system in question meets specific requirements.

child: A child is a human being defined as a child or minor by applicable laws and regulations, for the purposes of digital services provided within the context of IEEE Std 2089.1 (see also UN Convention on the Rights of the Child)..

children’s rights: A framework of legal and other obligations and ethical values covering civil, political, economic, social, and cultural rights afforded to every child.

NOTE—Documented in the United Nations Convention on the Rights of the Child.

child rights impact assessment: A tool predicting the impact of any proposed law, policy or budgetary allocation, which affects children and the enjoyment of their rights.

client: A stakeholder that acquires or procures a product or service from a supplier.

NOTE—Other terms commonly used for a client are buyer, customer, service, site, owner, purchaser, or internal/organizational sponsor.

¹³Information on references can be found in [Clause 2](#).

context of use: Intended operational environment for a system.

NOTE 1—The environment determines the setting and circumstances of all influences upon a system, including not only other systems but also people, settings, social, and ecological factors, etc.

NOTE 2—Context of use can be captured using a Context of Use Description (See ISO/IEC 25063.3[B2]).

control: The ability to determine the nature, sequence and/or consequences of technical and operational settings, behavior, specific events and/or experiences.

NOTE—Control includes cognitive control; that is being informed about activities; decisional control: having choices over actions; and behavioral control; receiving feedback from actions.

data minimization: Any data collected and/or processed should be needed to perform a specific action and limited to what is strictly necessary for the purpose for which it is being processed.

design: <process> To define the architecture, elements, interfaces, and other characteristics of a product, service or system, or system element.

design: <noun> Result of the design process.

environment: Context determining the setting and circumstances of all influences upon a system.

NOTE—Also applies to products and services.

ethical: Supporting the realization of positive values or the reduction of negative values.

NOTE—In this definition, a system can be ethical or unethical in the sense that it bears value dispositions to cater to positive value creation or negative value prohibition.

evolving capacity: This should be understood as an enabling principle that addresses the process of children's gradual acquisition of competencies, understanding, and agency. As children acquire enhanced competencies, there is a diminishing need for protection and a greater capacity to take responsibility for decisions affecting their lives.

NOTE—For additional clarification consult the section on evolving capacities in United Nations General Comment 25.

facial age analysis: Software that assesses the characteristics of a facial image at the pixel level using an artificial neural network to generate an age estimate.

facial recognition: Software that compares a stored facial image with a new image to confirm a match.

fair terms: A concept that the terms of use for a product or service do not put the consumer at a disadvantage.

false negative: An erroneous rejection of the hypothesis that a statistically significant event has been observed. This is also referred to as a type 2 error.

false positive: An erroneous acceptance of the hypothesis that a statistically significant event has been observed. This is also referred to as a type 1 error.

harm: (noun) A negative event or negative social development entailing damage or loss to people.

harm: (verb) Acting with negative value effects for self or others, within a respective product or service, organization, or beyond.

human rights: See Universal Declaration of Human Rights, United Nations General Assembly, 10 December 1948 (General Assembly resolution 217 A).

identification: The process of recognizing a particular user of a computer or online service.

information society service (ISS): Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

level(s) of assurance: A term used in identity standards for a combination of the Level of the Identity (see UK Government GPG 45) and the Level of Authentication (GPG 44). To avoid confusion with the term “age assurance” in IEEE Std 2089.1, and to avoid implying equivalent to the standards used in Identity, IEEE Std 2089.1 uses instead level(s) of confidence. *See: level(s) of confidence.*

level(s) of confidence: The varying combinations of accuracy, binding, certainty, liveness detection and authenticity that different solutions offer in establishing an age or age range.

NOTE—IEEE Std 2089.1 refers to the five defined levels of confidence for the age assurance processes for which it is anticipated will be defined in an ISO standard currently under development (see [Annex A](#)).

life cycle: Evolution of a system, product, service, project, or other human-made entity from conception through retirement.

life cycle model: A framework of processes and activities concerned with the life cycle that may be organized into stages, which also acts as a common reference for communication and understanding.

liveness detection: An algorithmic function designed to verify a biometric is from a live source, such as a human being and not from an imitation such as a wax replica, a picture, or a video.

liveness false acceptance rate: The proportion of unauthorized users (i.e., not a genuine, live human being) incorrectly accepted as being live.

online service: Anything accessed through the internet or through mobile communications systems or mobile devices.

operator: An individual or organization that performs the operations of a product, service, or system.

NOTE 1—The role of operator and the role of user can be vested, simultaneously or sequentially, in the same individual or organization.

NOTE 2—An individual operator combined with knowledge, skills, and procedures can be considered as an element of the service or system.

NOTE 3—An operator may perform operations on a product or service that is operated, or of a product or service that is operated, depending on whether or not operating instructions are placed within the product or service’s boundary.

organization: A group of people and facilities with an arrangement of responsibilities, authorities and relationships, for example, corporations, firms, enterprises, institutions, charities, a sole trader, associations, or parts or combinations thereof.

NOTE—An identified part of an organization (even as small as a single individual) or an identified group of organizations can be regarded as an organization if it has responsibilities, authorities, and relationships. A body of persons organized for some specific purpose, such as a club, union, corporation, or society, is an organization.

outcome error parity: Protected groups (as defined by law in each relevant jurisdiction) receiving an equal proportion of positive outcomes, or an equal proportion of errors.

parental attestation: The process whereby the age of a child is asserted by their parent or guardian

parental controls: Methods that control the online activity of children at the discretion of their parent or legal guardian, including parental attestation.

NOTE—Parental controls are not a form of age assurance.

personal data: Any information that relates to an **identified or identifiable individual**.

personally identifiable information: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

personal information: In US law, individually identifiable information about an individual collected online, including:

- a) A first and last name.
- b) A home or other physical address including street name and name of a city or town.
- c) “Online contact information,” as defined.
- d) A screen or username where it functions in the same manner as online contact information, as defined.
- e) A telephone number.
- f) A Social Security number.
- g) A persistent identifier that can be used to recognize a user over time and across different websites or online services. Persistent identifiers include, but are not limited to, a customer number held in a cookie, an internet protocol (IP) address, a processor or device serial number, or unique device identifier.
- h) A photograph, video, or audio file that contains a child’s image or voice.
- i) Geolocation information sufficient to identify street name and name of a city or town.
- j) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition. “Online contact information” means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

precision: The reproducibility of a measurement.

privacy preserving: A method of performing a process that does not lead to any more personal information being stored than the single piece of data required as output data. In the case of age assurance this could include a specific age, birth date, or age range.

process: A set of interrelated or interacting activities that transforms inputs into outputs (see ISO/IEC/IEEE 12207: 2008).

product: An artifact resulting from the execution of a process (e.g., age or age range).

project: An endeavor with defined start and finish criteria undertaken to create a product or service in accordance with specified resources and requirements.

requirement: See ISO/IEC/IEEE 29148:2018.

resource: An asset that is utilized or consumed during the execution of a process.

NOTE 1—Includes diverse entities, such as funding, personnel, facilities, capital equipment, tools, and utilities, such as power, water, fuel, and communication infrastructures.

NOTE 2—Resources include those that are reusable, renewable, or consumable.

reliability: The probability that a product, system, or service will perform its intended function adequately for a specified period of time, or will operate in a defined environment without failure.

relying party: An organization that has a requirement for age assurance.

risk: See ISO Guide 73:2009.

NOTE 1—An effect is a deviation from the expected—positive or negative. A positive effect is also known as an opportunity.

NOTE 2—Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

NOTE 3—Risk is often characterized by reference to potential harmful events and consequences, or a combination of these.

NOTE 4—Risk is often expressed in terms of a combination of the potential consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5—Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

sensitivity: An absolute quantity, the smallest absolute amount of change that can be detected by a measurement.

service: The performance of activities, work, or duties. This includes freemium services.

NOTE 1—A service is self-contained, coherent, discrete, and can be composed of other services.

NOTE 2—A service is generally an intangible product.

stage: A period within the life cycle of an entity that relates to the state of its description or realization.

NOTE 1—Stages relate to major progress and achievement milestones of the entity through its life cycle.

NOTE 2—Stages often overlap.

supplier: An organization that enters into an agreement with the acquirer for the supply of a product or service.

NOTE 1—The acquirer and the supplier sometimes are part of the same organization.

system: A combination of interacting elements organized to achieve one or more stated purposes. When this happens there shall be a clear separation between the two parts of the organization and data processed for age assurance may not be used for any other purpose.

NOTE 1—A construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, processes, and documents; that is, all things required to produce systems-level results.

NOTE 2—Other terms commonly used for supplier are contractor, producer, provider, seller, or vendor.

task: A required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a process.

trade-off: A decision-making action that selects from various requirements and alternative solutions on the basis of net benefit to the stakeholders.

top management: A person or group of people who direct and control the organization at the highest level.

NOTE—Top management can be the owner of an organization, majority shareholders, senior manager in the organization, or members of the governing board.

unfair terms: Terms that do not meet the definition of “fair terms.” *See also:* **fair terms.**

user: See ISO/IEC 25010:2011.

NOTE—The role of user and the role of operator are sometimes vested, simultaneously or sequentially, in the same individual or organization.

validation: See ISO 9000:2015.

value: Something desirable that influences the selection from available modes, means and ends of action. Examples of positive values include love, privacy, security, transparency, accountability, generosity, dignity, courage, and fairness. Examples of negative values include bias, ambiguity, absence of privacy, selfishness, and greediness.

4. Acronyms and abbreviations

AA	age assurance
AE	age estimation
AV	age verification
GC25	general comment 25
GDPR	general data protection regulations
UNCRC	United Nations Convention on the Rights of the Child

5. Conformance

The processes in this standard allow an organization to construct a life cycle and/or design, and to develop methodologies that can help make its product and services more age appropriate.

This standard can be used in one or more of the following modes:

- By an organization: to help establish appropriate age assurance processes. These processes can be supported by an infrastructure of policies, methods, procedures, techniques, tools, and trained personnel to support the organization to perform and manage its projects and systems through each of their life cycle stages. In this mode this standard is used to assess if the organization’s approach is conducive to effective age assurance outcomes.
- By an age assurance provider: to help select, structure, and employ the elements necessary to provide age assurance to organizations. In this mode, this standard is used to determine the client organization’s requirements and assess if the project’s outcome is effective in applying age assurance to the level required by applicable laws or regulations or publicly promised, while promoting the principles of privacy, security, equity and children’s rights.
- By a prospective client: to help develop an agreement concerning processes and activities that deliver age assurance. Via the agreement, the processes and activities in this standard are selected, negotiated, agreed to, and performed. In this mode this standard is used for guidance in developing agreements referring to age assurance to the level of assurance required by applicable laws or regulations or publicly promised, while promoting the principles of privacy, security, equity and children’s rights.
- By process assessors: to serve as a process reference model for use in the performance of process assessments that may be used to support organizational process improvement for digital services and products that engage with children.

There is only one criterion for claiming full conformance—full conformance to both outcomes and tasks. Full conformance to outcomes and tasks is achieved by demonstrating that all the outcomes and the required activities and tasks in [Clause 8](#) through [Clause 14](#) and with associated information in [Annex A](#) and [Annex B](#) have been achieved. The inputs and outputs shown in [Clause 7](#) through [Clause 14](#) are not requirements except as specifically required in the activities and tasks. The inputs are informative, and the outputs are normative. The inputs and outputs are demonstrable predictors of the outcome in each process.

Conformance can only be achieved if the provider and the client observe the full requirements of the standard.

6. Key concepts and application

6.1 General application

This standard is usable by organizations that engage in system and software engineering and product and service design and development. This includes the following in particular:

- a) Organizations providing services and products that engage with children or are likely to be accessed by or engage with children, either directly, indirectly, deliberately, or in the course of their operations.
- b) Organizations building a new generic or application-specific online service from scratch that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations.
- c) Organizations implementing a major revision on an existing product, service, or system that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations.
- d) Organizations planning the acquisition of a tailored product, service, or system that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations.

NOTE—Children’s Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq. and Children’s Online Privacy Protection Rule 16 CFR Part 312 should be considered in the USA.

- e) Organizations providing services and products they wish, or are legally required to, help prevent all children or children of a specific age or age range accessing them.
- f) Organizations providing services and products they wish, or are legally required to, deliver age specific benefits to all children or children of a specific age or age range (paywall news service or children’s news programming).
- g) Research organizations (including universities) that build a new product, service, or system from scratch or adapt an existing entity in the course of their research activities that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations.

Application may be to the entirety of a service, or only to parts of it where age assurance is required.

6.2 Specified context of use

Many organizations engage with children intentionally, others engage with children in the course of their general activities. Some impact on children without engaging directly with them, and some engage unintentionally. In some cases, age assurance may be a legal requirement, in other cases implemented voluntarily to better tailor the service to children, by providing age-appropriate instructions for use, or disabling risky features. Age assurance may not be necessary. When being implemented, the level of assurance required should be proportional to the assessed risk in all cases. Users should consider whether to use more robust age assurance if not required by law or regulation. This standard sets out the methodology of interrogating the service from the point of view of the established rights and needs of children and provides any organization a starting point from which to implement age verification.

In addition, systems shall be compliant with relevant national and regional legislation and industry standards in the jurisdiction(s) in which the service or the product is offered and from which users are accepted, and a listing of such jurisdictions should be maintained. Services and products that are offered in more than one jurisdiction shall comply with all applicable laws and regulations in each jurisdiction where they are offered and from which users are accepted, and be transparent where the service or product is different in different jurisdictions, including the following:

- Children’s rights as set out in the United Nations General Comment 25
- Data protection regulations, including regulations that protect children’s data specifically, such as the Age-appropriate Design Code (UK) and Age-appropriate Design Code Act (California)
- Consumer legislation
- Equality legislation
- Legislation that covers treatment of children (for example, education, health, justice)
- Health and safety legislation
- Such regulations and legislation that protect children and promote their rights in any jurisdiction
- Accessibility legislation

6.3 The organization

This standard is intended to be used in systems and software engineering and digital services organizations of all types and sizes, whether they apply a hierarchical or a relatively flat organizational model. It is also usable by components of an organization, such as a product development team or a corporate division, although

conformance to the standard will likely require participation across organizations in an integrated value/supply chain. It is intended for local, regional, national, or international use with various cultural values and governance systems.

In applying this standard, one person can assume many roles, and one role can be held by numerous individuals or subgroups within the organization. The duties associated with all roles shall be fulfilled.

Age assurance may be provided by an independent third party to the organization that is the relying party. If it is provided internally by the relying party itself, all elements of the relying party's management, systems, and data that are involved in these processes must be clearly identified and fall within the scope of this standard. Where these are not clearly separated from other systems, all parts of the system are within scope.

Design and service provision decisions that impact children are not the sole responsibility of top management, although top management has an undeniable role in setting expectations for organizational values and priorities and establishing control of performance and final outcomes. This standard requires that systems and software engineers shall use informed judgment while making design decisions about a system under development and such decision may not be left solely to management. Both engineers and others in the organization, including those with responsibility for compliance, can benefit from learning and regularly applying specific processes and methods to apply age assurance throughout the life cycle. Just as engineering analyses, decisions, and risk assessments have always involved balancing and tradeoffs of priorities and values, in this context, engineers participate as the organization balancing and finding solutions for competing interests (e.g., risks/harms). Although involvement with internal or external experts (e.g., in child rights or child development) may improve outcomes and efficiency, it is not required to engage an expert to conform with the standard. Whether or not an internal or external expert is involved, it remains the case that all adults in all roles when balancing the tradeoffs shall conform to the principle that the best of the interest of the child is paramount, per General Comment 25. Where a conflict arises between the commercial interests of a company and a child's it is vital that the company shall consider the best interests of the child as a priority. The commercial interest of a company should not take precedence over the best interest of the child.

6.4 Stakeholders

There may be a wide range of stakeholders involved in the products and services that impact children. Internal stakeholders include the many roles required to commission, develop, build, and market products and services. Primary stakeholders include, for example, a child, groups of children, parents, educators—and often adults. There may be third parties that have specific interests, for example, an owner or developer of an app will have an interest and be affected by an app store's policies and practices, a regulator, a trade association to whom the system owner is accountable, or third parties that may seek to benefit from data associated with age assurance.

Additionally, there are those who interfere or exploit digital systems, such as hackers, scammers, or predators. These groups of negative stakeholders can often have an asymmetric influence on the design of the product. An asymmetric influence means having more power to assert the stakeholders' interests and views.

Typically, those connected with the proprietary ownership of the technology are the most influential and the end user may only have the power to reject or accept the product or service in its entirety. In the case of age assurance, it has long been the case that some children have been offered a take it or leave it service. In the case of systems that impact a user without their knowledge, for example by obtaining their data from a third party, they may have no influence at all. This power imbalance is particularly acute when the end user is a child or if no alternative service is on offer.

This standard offers a set of processes that engage stakeholders with each other to apply age assurance to a product or service in a way that prioritizes the rights and needs of children. The person(s) or company building the product or service can, by following this standard, identify the risks and benefits of their system to children and take steps to mitigate risks, amplify benefits, and keep both under review. This set of processes does not seek to undermine engineering realities, nor does it offer an aspirational or perfect world for children,

rather it offers actions that, if followed, can help to make age assurance products more private, more secure, more equitable, and proportionate to circumstance. They describe a floor of compliance and not a ceiling of ambition. It is anticipated that smaller or newer companies will seek to adopt or purchase age assurance systems built by others. In that instance, they should adopt certified products or products that come from trusted sources that meet the criteria set out in this standard and have been approved by competent regulating authority, where applicable.

6.4.1 Children as users

Along with these internal stakeholders and the customer, the class of stakeholders that is intrinsic to age assurance is the user, in this instance, a child. Children want, like, and need to use digital services and products, and age assurance is a tool that can be used to offer them differentiated access to services and products. There cannot be a presumption that children are able to assess the risk or benefits of use of any system nor that providing “more information” is in itself a sufficient response to offering an age-appropriate service, informing them of their rights, or trying to meet their needs. Nor can it be assumed that all children have a parent or adult in loco parentis who is engaged, literate, skilled, or able to act on their behalf.

Age checking does not mean that the service or product has been designed to be age appropriate, which is best set out in IEEE Std 2089™ covering how to build an age-appropriate digital services. Companies that have taken a child rights approach to age assurance can be the same companies that are also beginning to consider the needs and development capacity of their child users.

Users frequently are categorized by the levels or types of system access and permissions they need to perform various tasks, or have services provided to them. These include the hands-on system operators (often agents of the customer) as well as those who benefit from or are harmed by use of the system, both through direct transactions using the system and through its impact on the environment and their culture. The word “users” here also includes those who access a system, whether or not they share data with it beyond the age assurance process itself.

Not all children are the same, and children of different ages, contexts, ethnicity, capacity, and socioeconomic groups may require different levels of support or consideration. In this context, “capacity” means the cognitive ability to comprehend materials plus the ability to be able to read materials. For example, designers need to take particular care that the system design and algorithms do not unjustifiably favor or select users in certain geographic areas, of certain biometric or demographic characteristics, or based on unvalidated reports and unfairly target or exclude other classes of users.

6.4.2 Who can threaten or support the best interest of the child?

Another class of stakeholders may have interests that oppose the system or may interfere with its use. These include competitors, cybersecurity hackers, or opponents of the organization, system owner, or customer. There is also a significant group of producers and consumers of child sexual abuse material. Other external stakeholders can offer divergent perspectives. Government regulators and external advocacy groups, whose expertise, cultural norms, and values may differ from the system owner, can expose a clash in values or demand a higher bar of safety or benefit for children. These conflicting and often oppositional values may even constrain and/or aid the decisions of the system owners that are a direct threat to the needs, rights, and values of children.

To help counteract any threats to children, the organization may consider the use of the third-party assessors, data brokers, and independent certification and validation contractors. These are other types of stakeholders who can point out flaws or unstated assumptions that have influenced or skewed the organization’s ethical choices against the needs, rights, and values of children.

This standard helps to identify how internal and external stakeholders, users, opponents, and independent authorities can be treated differently when age appropriateness and risks are evaluated. Information about

potential system characteristics and performance and the balance of values and stakeholder interests are rarely shared openly with all stakeholders. Therefore, it is one of the goals of this standard to present a set of processes that helps organizations better understand this obfuscated balance of interests and values while a child's best interests are paramount.

6.5 Stages and processes

This standard allows any organization, systems developer, or digital services provider to provide age assurance by means of their own set of standard system development processes, methods, and practices. Provided the outcome matches the stated aims of each stage or process. These may be specific to the needs of this standard or relate to the general processes in ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017.

This standard is intended to be suitable for use by organizations and software projects using iterative approaches and methods, as well as in those using other formal engineering approaches.

The activities and tasks in this standard are not sufficient by themselves to produce a product or service that is age appropriate. They are intended to verify that the process of age checking is more private, more secure, more equitable and rights respecting.

This standard does not prescribe a sequence of processes within the life cycle model. However, many of the activities and tasks logically apply outputs from other tasks, so there is an inherent sequence of activities that can be applied iteratively. The sequence of the processes is determined by project objectives and by selection of the life cycle model. But to conform to the standard, all processes shall be undertaken and achieved.

7. Roles and responsibilities of key actors in the age assurance process

7.1 General

There are many roles required to successfully complete the tasks and activities outlined in this standard. The roles and their associated competencies that shall be fulfilled are documented in 7.2. These roles may be assigned to one or many people so long as the workload, competencies, and accountabilities are all met.

Whether the age assurance is provided by a third party or a relying party acts as its own age assurance provider, approaches shall be open to independent scrutiny. In the case of a relying party operating their own age assurance system, then the age assurance operations shall be maintained at arm's length to be sufficiently distinct to meet all the requirements of this standard, i.e., that the age assurance process is undertaken independently of the relying party's core operations and free of actual or perceived conflict of interest. It may be necessary to establish operations at arm's length from the rest of the service to meet unequivocally the requirements of this standard. In both cases, third party or internal age assurance, there is a responsibility that these processes are transparent, open to independent scrutiny and measurable against the requirements of this standard. This may be achieved by independent audit leading to certification and may be subject to further scrutiny by relevant regulators.

7.2 Role descriptions

7.2.1 Relying party

The relying party is an information society service (ISS) offering goods, services, or content to users online.

The responsibilities of the relying party shall include the following:

- a) Determining and documenting the need for age assurance, of all or specific elements of the service; including the age or age ranges and the reasons for action including regulatory or corporate social responsibility.
- b) Assessing the level of confidence required for each element of the service.
- c) Developing age assurance technology or selecting one or more third-party age assurance (AA) providers that meet all requirements and processes set out in this standard.
- d) Implementing age assurance.
- e) Maintaining the independence of the age assurance process from other aspects of its management, systems, and operations.
- f) Monitoring the effectiveness of age assurance.
- g) Maintaining conformance with this standard.
- h) Verify that third party agreements or technical implementation of the age assurance provider technology does not in practice undermine any aspect of this standard.

NOTE—It is not a requirement of this standard but it is desirable that companies should also meet IEE Std 2089™ so that their service can be more age appropriate—once age has been established.

A relying party should have the following competences:

- An understanding of relevant data protection legislation
- Ability to run a technical procurement process or to specify technical requirements for in-house developers

7.2.2 Age assurance provider

The age assurance provider is either an internal or external third-party supplier of technology to estimate or verify the age of an online user.

The responsibilities of the age assurance provider shall include the following:

- a) Develop system/software requirements that enable age assurance that meets all of the requirements and principles set out in this standard.

NOTE—This should include consideration of children’s views, as set out in article 12 of UNCRC, and meet the requirements of General Comment 25 most particularly, a right to privacy, the freedoms of association and speech, and protection from both material and immaterial harm.

- b) Advise the relying party on age assurance options, advantages, and disadvantages to allow it to meet its legal responsibilities and comply with the regulatory requirements likely to apply in the jurisdictions where it operates.

NOTE—The legal responsibility for compliance generally remains with the relying party.

- c) Advise the relying party on suitable methods of age assurance in the context of approaches available in the marketplace and the relying party’s business and existing data.
- d) Advise the relying party on the appropriate levels of confidence required in proportion to the risks of harm identified by the relying party, where these are not specified by law or regulation.

- e) Advise the relying party on the established rights of children, as set out in GC25, noting in particular their rights to privacy, security, protection from harm (economic, physical, and emotional) as well as their rights to free association and speech.
- f) Operate age assurance.
- g) Maintain the privacy of user data, as well as the security, accuracy and integrity and proportionality of the age assurance process.
- h) Verify that relying parties implementing the provider's technology also meet the requirements and principles of this standard.

NOTE—The term “previous age assurance provider” is used in the interoperability phase to describe an age assurance provider which has already completed an age check for a user, allowing the user to re-use the same check with another relying party or age assurance provider in future.

An age assurance provider should have the following competences:

- Technical ability to create or integrate components required to complete age assurance checks
- Understanding of relevant data protection legislation
- Ability to implement a high level of data security

7.3 User

The user is a person wishing to access the relying party.

The responsibilities of the user shall include the following:

- a) Supply on request if required appropriate evidence as an input to the age assurance process.
- b) Participate in the authentication process that may be required as part of the age assurance process or to re-use a previous age assurance check.
- c) Determine through giving or withholding consent the extent and manner to which an age check may be re-used by the same or other relying parties.

No competences can be assumed of a user.

8. Determining the need for age assurance (“determination phase”)

8.1 Purpose

The purpose of this process is to undertake an initial overview of a service or product and identify the statutory, regulatory, contractual, and ethical requirements for age assurance.

8.2 Outcomes

When the determination phase has been successfully implemented, it shall be possible to show the following for age assurance:

- a) The age or age range of the children to with the relying party is engaging.
- b) The level of risks of the relying party's service, or parts of the service, poses for children of that age or age range that they shall, should or may need to mitigate.

- c) Any statutory requirements for the relying party or age assurance provider in each of the jurisdictions where its services or products are offered or from which users are accepted in which age assurance plays a part. Relying parties may choose not to exit a jurisdiction based on compliance requirements, in which case this should be documented.
- d) Any regulatory requirements for the relying party in each of the jurisdictions where its services or products are offered or from which users are accepted in which age assurance plays a part. Relying parties may choose not to offer services or products in or not to accept users from a jurisdiction based on compliance requirements, in which case this should be documented.
- e) That contractual requirements for the relying party arising from any agreements it has entered into are consistent with this standard.
- f) The policy and ethical requirements of the relying party, including, but not limited to, its published terms (including terms and conditions, privacy notices, community guidelines), or as determined by its board or a nominated delegate of the board.
- g) That children's best interests were considered paramount in instances where there were conflicting interests, and document any instances where children's best interests did not prevail.

NOTE—This stage should include consideration of children's views, as set out in article 12 of UNCRC, and meet the requirements of GC 25 most particularly, a right to privacy, the freedoms of association and speech, and protection from harm.

8.3 Activities and tasks

The project shall implement the following activities and tasks to determine the need for age assurance as follows:

- a) Identify all jurisdictions where users are located.
 - 1) Establish the age or age range of users that are accessing the relying party service.
 - 2) Identify the level of risks to the service or parts the relying party poses for children of that age or age range that they shall, should or may mitigate.
 - 3) Analyze existing site traffic data to assess in which jurisdictions users are located, or identify jurisdictions where the relying party expects to have users if it is not yet operational there.
 - 4) Assess the scale and location of the backlog or pre-existing user base as well as new users.
- b) Decide in which jurisdictions the organizations wishes to comply with laws and regulations.
 - 1) This may be informed by the next step, so the decision can be informed by the potential requirements in any jurisdiction where the relying party operates.
 - 2) Where legal, limit access to users to jurisdictions where the relying party can or decides to achieve compliance with relevant law and regulations, and this standard, as far as is technically feasible.
- c) Identify the applicable statutes and regulations for each jurisdiction where compliance is deemed a requirement.
- d) Review all third-party contracts to identify any obligations relating to age assurance.
- e) Specify the levels of confidence and service levels required for each element of the relying party in proportion to the risks of harm identified by the relying party, where these are not specified by law or regulation or contract.
- f) The board or its delegate may determine that the relying party requirements relating to age assurance may extend beyond those already demanded by statute, regulation or contract.

- g) Determine when it is necessary to repeat this phase by the following:
 - 1) Defining a regular review by time period which should be at least annual.
 - 2) Implementing surveillance for critical changes in law and regulation in the jurisdictions in scope.
 - 3) Identifying internal triggers, such as a launch of a new product, or expansion into a new jurisdiction, and implement or amend existing processes to prompt the repetition of this phase.
- h) Document the need for age assurance with clear cross-referencing to each of the items in this list in an age assurance practice statement.

8.4 Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

- Relying party user traffic data
- Current user onboarding flow, user experience, user interface, communication channels
- Statutes
- Regulations
- Relying party contracts database
- Business strategy (including any business model and geographical expansion plans)
- Marketing plans
- Product development processes and plans
- Relevant existing policies of the relying party e.g., accessibility, inclusion
- Child rights impact assessment

8.5 Outputs

The following work products constitute a suitable, but non-exhaustive suite of the process deliverables:

- Age assurance practice statement (Part 1—Determination)

9. Selecting the method(s) of age assurance (“selection phase”)

9.1 Purpose

The purpose of this process is to select the most appropriate method or methods of age assurance that meet the standards for age assurance set out in [Annex A](#).

9.2 Outcomes

When the selection phase has been successfully implemented, it shall be possible to show the following:

- a) The methods of age assurance the relying party will implement to comply with its age assurance practice statement.

NOTE—More than one method may be made available, and either offered as a choice to the user or selected by first using a primary method and then providing fallback options selected based on a waterfall, with additional

methods deployed when a method fails to determine the age or age range to the level of confidence required. Ideally a variety of methods should be part of the implementation so that those without hard identifiers or those with protected characteristics can access the service.

- b) That each method meets the privacy and security standards for age assurance set out in [Annex A](#).
- c) That the level of confidence achieved by each method is proportionate to the risk profile.

9.3 Activities and tasks

The project shall implement the following activities and tasks to select the methods of age assurance as follows:

- a) Identify the level or levels of confidence required for age assurance.
 - 1) With reference to the age assurance practice statement (Part 1—Determination), the relying party shall define one or more levels of confidence required.
 - 2) The relying party may obtain personal data from a user when the user first accesses it, which may be indicative of age. If obtained for the purpose of age assurance, this data shall not be reused for any other purpose nor shared or sold.
 - 3) The relying party may seek additional personal data from the user to establish age or age range in any manner, including but not limited to biometric, hard identifier, behavior, provided that this information once used for this purpose is not shared sold repurposed or analyzed for any other purpose.

Where this is necessary, the relying party should consider what user data can be obtained, based on the nature of the relying party, the user and the hardware involved. The collection of biometric or behavioral information may subject the relying party to additional legal requirements. Review of relevant laws and regulations shall be conducted when new types of information are collected.

- 4) The relying party shall seek the minimum personal data required to achieve an age assurance to the level of confidence required and describe the data processed in published terms.
- 5) Personal data obtained for the purpose of age assurance shall not be used for other purposes, to maintain confidence in data security and privacy when age assurance is required.
- 6) Select the method or methods of age assurance that are most suited to the available or potential data and that deliver the required level of confidence.
- 7) The relying party shall consider the range of methods available that deliver age assurance that meet the minimum standards and deliver the level of confidence (which is itself a combination of accuracy, reliability, binding, authentication and liveness as set out in [Annex A](#)) required by the relying party. Such methods may include age verification or age estimation, where consistent with applicable laws and regulations.

Age estimation inherently involves a high level of binding. An appropriate buffer may be used so that the age estimated (also known as “the challenge age”) is sufficiently different from the required age to meet the required level of confidence, for example if a child needs to be a certain age to use a service, it may be necessary to only allow those children estimated to be a certain amount over that age, or where there is a requirement it may be necessary to set the buffer so that almost all users are over that age.

Where the user’s age is too close to the required age or otherwise to allow age estimation to meet the standard, methods of age verification which are based on the specific date of birth of the user shall be required. Database verification using government or equivalently authoritative information sufficient to confirm the age of the individual, document authenticity, liveness detection, and facial matching may be stipulated for adequate confidence.

- b) Confirm that each of the selected methods of age assurance and the user flow within the relying party meet the standards for age assurance in that they:
- 1) Protect the privacy of users, in compliance with data protection laws, regulations and obligations under any treaties enforceable in any relevant jurisdiction, including those listed in item 11) .
 - 2) Are proportionate having regard to the risks arising from the product or service and to the purpose of the age assurance system.
 - 3) Offer functionality appropriate to the capacity and age of a child who might use the relying party.
 - 4) Are secure, and shall not expose users or their data to unauthorized disclosure or security breaches.
 - 5) Does not use data gathered for the purposes of the age assurance system for any other purpose.
 - 6) Provide appropriate mechanisms and remedies for users to challenge or change decisions if their age is wrongly identified.
 - 7) Are accessible and inclusive to users with protected characteristics.
 - 8) Do not unduly restrict access of children to services to which they should reasonably have access, for example, news, health and education services, in line with the UN Convention on the Rights of the Child.
 - 9) Provide sufficient and meaningful information for a user to understand its operation, in a format and language that they can be reasonably expected to understand, including if they are a child.
 - 10) Are effective in verifying the actual age or age range of a user as required.
 - 11) Do not rely solely on users to provide accurate information, unless an asserted level of confidence is proportionate to the risks of harm.
- c) Are compatible with the following:
- 1) Data protection legislation, in particular the principle that the minimum amount of data necessary is collected, and of any codes published by regulators in respect of the processing of children’s data.
 - 2) The Universal Declaration of Human Rights.
 - 3) Any equalities legislation.
 - 4) The United Nations Convention on the Rights of the Child and General Comment No. 25 (2021) on children’s rights in relation to the digital environment.

NOTE—This subclause applies to all age assurance systems irrespective of the system’s size, nature, or approach. These may be independently operated by a third-party, supplied by an AA provider (acting as the provider’s agent) or those where a relying party operates an internal but distinct system to conduct age assurance.

9.4 Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

- The Universal Declaration of Human Rights
- The United Nations Convention on the Rights of the Child
- General Comment No. 25 (2021) on children’s rights in relation to the digital environment
- Existing user data analysis
- Hardware assessment

- Child rights impact assessment
- Comprehensive understanding and research on available and emerging age check technologies

9.5 Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

- Age assurance practice statement (Part 2—Methods)

10. Assuring the age of a user (“assurance phase”)

10.1 Purpose

The purpose of this process is to undertake assurance of the age or age range of each user of the relying party where age assurance is required by the age assurance practice statement (Part 1—Determination), doing so in accordance with age assurance practice statement (Part 2—Methods).

10.2 Outcomes

When the assurance phase has been successfully implemented, the relying party shall be able to show the following:

- That the age or age range of each user accessing age-restricted goods, services, or part of service to the level of confidence meets the age restriction set out in the age assurance practice statement

NOTE—The level of confidence required may be different for users of different ages and or for different elements of the same service. (Part 1—Determination).

10.3 Activities and tasks

The age assurance provider shall implement the following activities and tasks to determine the need for age assurance as follows:

- a) Receive the request for age assurance from the relying party, which shall include a copy of the age assurance practice statement in order to establish some or all of the following:
 - 1) The most appropriate age assurance method(s) to implement
 - 2) If required the format in which age is to be established e.g., date of birth, age in years or age range or age above, or age below
 - 3) The level of confidence required
 - 4) The level of authentication required
 - 5) Whether a specific date of birth must be part of the process
 - 6) The agreed set of primary and fall back methods for each jurisdiction.
 - 7) A unique (encrypted/hashed) identifier for each age check request
 - 8) Any user data that the relying party has already legally acquired about the user that is required for the age verification method(s) selected in order to not duplicate demands for data.
- b) If the user has already completed an age assurance process using the age assurance provider, or a provider with which it is interoperable, whether internal or third party, that meets the requirements

of this standard, and the level of confidence, authentication, and exactitude needed by the relying party, the law and regulation of the jurisdictions in which it is to be re-used and is limited only to sharing the attribute of age, then it may be used as confirmation of age. This provision may not be used to undermine, water down, or avoid full conformance with this standard, the companies own responsibilities nor any jurisdictional legal differences.

- c) Advise the user in a meaningful and age-appropriate way that they need to establish their age and their right and method to challenge any mistakes that have been made.
- d) Identify an approved data protection basis to undertake the current age check, and for any subsequent checks on the appropriate data protection basis.
- e) Transparently obtain any further user data required for the selected methods of age assurance bearing in mind that age checking shall only process data necessary to perform the age assurance, shall not repurpose, share, or sell the additional data, and shall delete everything except the required age or age-range data, consistent with applicable laws and regulations.

To conform to this standard, an age assurance provider and a relying party shall not make age checking conditional on the provision of other information.

This may include a document with full name, date of birth, address, a facial image, a voice sample, behavioral data, subject always to the application of the principle of data minimization.

- f) Complete age assurance.
- g) Record an audit trail as required by legislation, regulation, contract, or policy. Audit trails shall not store personal data unless this is a legal requirement. The relying party shall document what data is retained and how it is secured.
 - 1) Transmit result and any required meta data that does not constitute personal data to the relying party according to applicable regulatory and audit requirements, including requirements for security of the data in transit.
 - 2) Results shall be provided as “yes” or “no” replies to the question as to whether the user meets the age or age-range requirement specified by the relying party where that is all that is required. Only where a regulator legally requires the date of birth shall this be provided.
- h) Delete all user data not required to enable future reuse or required by specific legal provisions.
- i) Provide each user with the right, and a process by which, to challenge the conclusion of the age assurance provider.

10.4 Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

- Requests for age assurance from the relying party
- User data
- Age assurance provider technology
- Age assurance practice statement

10.5 Outputs

The following work products constitute a suitable, but non-exhaustive suite of the process deliverables, subject to the application of the principle of data minimization:

- A response in the form of “pass” or “fail” for each user where age assurance is required
- A further response if required in the agreed form of either a date of birth, age is over, age is under or age range is within
- A confidence indicator for the result, as set out in [Annex A](#) based on the method(s) and solution used
- The level of outcome error parity to demonstrate the extent to which protected groups are receiving an equal proportion of positive outcomes, or an equal proportion of errors
- Details of failed checks (when a user did not pass), the reason for failure
- An audit trail with meta data of age assurance checks completed, by which method, or combination of methods, which shall not include any user data
- A timestamp of the response in UTC
- The signature of the complete response, digitally signed by the AA provider
- An auditable list of all types of data processed, what was deleted and what data was stored, including the intended time it will be stored for
- An overview of the measures used to secure data, both in transit and at rest

11. Categorizing the level of confidence with which the assurance has been completed (“categorization phase”)

11.1 Purpose

The purpose of this process is to categorize the level of confidence to which the assurance has been completed. There are four defined levels of confidence: asserted, basic, standard, and strict. These offer increasing confidence in the accuracy, currency, reliability, and other dimensions of confidence, but distilling the many potential combinations into four options to allow for better understanding and to facilitate interoperability across use-cases.

11.2 Outcomes

When the categorization phase has been successfully implemented, it shall be possible to show the level of confidence the age assurance provider and/or relying party has in the age of each user whose age has been verified.

11.3 Activities and tasks

The project shall implement the following activities and tasks to categorize the level of confidence with which age assurance has been completed as follows:

- Assess any existing certification for the age assurance providers technology against the requirements of this standard, including, but not limited to, children’s rights to privacy, participation, and protection.
- Undertake performance tests for uncertified technology against the requirements of this standard.
- Categorize the result against the levels of confidence in [Annex B](#).

11.4 Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

- Levels of confidence for age assurance listed in [Annex B](#)

11.5 Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

- A certified record of the level of confidence for each method of age assurance that is being provided, both individually and when working together.
- The age assurance provider or relying parties shall not create a database of responses based on checks carried out by previous age assurance providers or relying parties.

12. Exchanging the results of age assurance checks with other organizations (“interoperability phase”)

12.1 Purpose

The purpose of this process is to allow an age assurance provider to exchange the results of an age assurance process with another age assurance provider in a privacy preserving fashion and in the best interest of the child, consistent with all applicable laws and regulations.

12.2 Outcomes

When the exchanging phase has been successfully implemented, it shall be possible to show the following:

- The certification required to allow other age assurance providers or relying parties to rely on age checks
- The ability to export age assurance checks
- The ability to import age assurance checks
- A narrative or technical statement that shows how sharing age information has not breached data minimization principles, does not create digital footprint for the child, and is sharing only the attribute of age and associated level of confidence

12.3 Activities and tasks

The project shall implement the following activities and tasks to determine the need for age assurance as follows:

- a) Achieve certification for each method of age assurance deployed that meets all requirements of this standard.
- b) Send requests.
 - 1) Requests shall be made by redirecting the user to a previous AA provider.
 - 2) The age assurance provider shall pass on the request from the relying party to the previous provider.

- 3) Where the age assurance provider is also a relying party, verify by written statement that the exchange does not in effect, either deliberately or unintentionally, create a digital footprint for the child that combines age with other information or shares more than the attribute of age or age range as requested.
- c) Receive and validate requests.
 - 1) The previous AA provider shall receive the request when the user is redirected to it, and it will then authenticate the user, and confirm there is a valid age check on record which meets the level of confidence required.
 - 2) Age checks shall not be valid for longer than the maximum period for each level of confidence.
- d) Provide responses.
 - 1) The previous AA provider shall provide a response to the AA provider in the same form as the response is then provided to the relying party.
 - 2) The previous AA provider shall not supply the date on which the age check was validated to help prevent the AA provider creating a database of responses based on checks carried out by previous AA providers (because the AA provider will not have knowledge of whether the check remains valid or has expired).
- e) Record volumes of requests sent and received by AA provider.
 - 1) Both the AA provider and the previous AA provider shall record the volume of checks at each level of confidence exchanged between them.
 - 2) To improve privacy, none of the previous records should contain personal information of the end-users involved.

12.4 Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

- Age assurance records
- Protocols for the secure exchange of requests and responses, including the language, fields, validation, etc., required to maintain the integrity and independence of the age verification (AV) process
- An exchange statement, which describes the approach of the age assurance solution to interoperability
- Comparisons between conformance with this standard and other certifications schemes

12.5 Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

- An API capable of sending and receiving age checks
- Results of age checks undertaken by previous AA providers

13. Protecting the privacy of users when undertaking age assurance (“privacy phase”)

13.1 Purpose

The purpose of this process is that age assurance solutions protect the privacy of users by design.

13.2 Outcomes

When the privacy-by-design phase has been successfully implemented, it shall be possible to show the following:

- The age assurance provider does not pass on attributes of the user other than date of birth, age range or age in the agreed format.
- The age assurance provider does not store any personal data after the age assurance has been completed beyond what is strictly necessary to comply with the law or where necessary to provide ongoing age assurance.

NOTE—Any stored data should be minimized, stored for the shortest amount of time necessary and stored securely.

- Where relying parties are given access to the full identity of the user it must be strictly for purposes that are required by law.

NOTE—In general requests from relying parties that require the full identity should not be considered age assurance but instead should be considered Identify verification.

- Relying parties shall not receive personal data about a user, beyond the age information.

13.3 Activities and tasks

The project shall implement the following activities and tasks to determine the need for age assurance as follows:

- Document the method by which age assurance transactions are recorded to confirm that it is not possible for the relying party to identify the user, and it is not possible for the AA provider to record which relying parties enquired about which of its users.
- Document how any disclosure of identity is separate from and blind to general age checking in which age is the only attribute shared.
- Apply ethical privacy criteria.

13.4 Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

- Age assurance provider system design documentation

13.5 Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

- Age assurance practice statement (Part 3—Child Data Privacy Impact Assessment)

14. Securing data relating to users used when undertaking age assurance (“data security phase”)

14.1 Purpose

The purpose of this process is to ensure that any personal data used during age assurance or retained after an age assurance has been completed is stored securely, in accordance with all applicable laws and regulations.

14.2 Outcomes

When the data security phase has been successfully implemented, it shall be possible to show the following:

- Data minimization with the only personally identifiable data stored being necessary either to comply with the law, or for the purpose of ongoing age assurance
- Data security to robust and secure industry standards such as the payment card industry data security standard
- Each user retains control over their personal data retained by the AA provider
- Evidence that the system is not vulnerable to penetration

14.3 Activities and tasks

The project shall implement the following activities and tasks for the security of personal data as follows:

- Document data flows and stores
- List attack vectors
- Conduct risk assessment
- Conduct penetration testing
- Complete mitigation activity
- Monitor ongoing network activity

14.4 Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

- Certification to data security standards
- Results of penetration testing
- Certified, age-appropriate report and redress system

14.5 Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

- Age assurance practice statement (Part 4—Data Security Certification)
- Penetration test results
- Report and redress system

Annex A

(normative)

Five standard levels of age assurance derived from six indicators of confidence in age assurance output

A.1 Indicators of confidence

The indicators of confidence associated with an age attribute to which the asserted age is confirmed by an age assurance system are defined in this normative across six dimensions:

- The accuracy of the outcome (4 levels)
- How frequently age assurance takes place (4 levels)
- The extend of counter-fraud measures (3 levels)
- The authenticity of the user (4 levels)
- How frequently authenticity is checked (4 levels)
- Whether the specific birth date is used and/or retained in the process (3 levels)

The levels for each dimension are each described in more detail in [A.2](#) through [A.8](#). (See also [Table A.1](#).)

The indicators of confidence of an age assurance check can be used by policy makers and regulators, or an organization, to set an age verification policy and by AA providers to describe the capabilities of their solutions, which can also be independently tested and certified against these levels.

Five normative combinations of these six dimensions can then be defined (asserted—basic—standard—enhanced—strict) as the “levels of age assurance,” which are recommended by the age assurance industry in the interests of simplicity and interoperability. There is no requirement to use only these five combinations as each use-case is distinct, with legal, cultural, and practical considerations that may compel an increase or decrease in the level specified in one or more dimension, but where possible, such exceptions should be avoided.

Where a solution uses more than one method of age assurance, often referred to as a “waterfall” approach, the whole system should be assessed as one to give an overall indication of confidence, which assumes the system is used to its full capability.

Table A.1—Levels of age of assurance

Level of age assurance	Accuracy	Duration	Counter-fraud	Authenticity	Authenticated	Illustrative only: potential use cases
Strict	Strict	Weekly	Resolved	Level 3	Each use	Purchase an offensive weapon
Enhanced	Enhanced	Monthly	Resolved	Level 2	Each use	Online gambling (exceptionally with the date of birth used and retained)

Table continues

Table A.1—Levels of age of assurance (continued)

Level of age assurance	Accuracy	Duration	Counter-fraud	Authenticity	Authenticated	Illustrative only: potential use cases
Standard	Standard	Annual	Communicated	Level 1	Monthly	Access pornography
Basic	Low	Indefinite	Communicated	Level 0	Annually	Access content that is not of significant harm, but is intended for older children.
Asserted	None	Indefinite	None	Level 0	Indefinite	Sign up to receive a kids' website newsletter containing content appropriate for all ages

Note that these normative levels of age assurance do not consider the use of a specific birthdate that can be applied to each if required by regulators (e.g., for online gambling).

The five normative levels of age assurance (see [Table A.1](#)) should be considered first before making any specific adjustments to the level required on one or more dimension. There are then 768 permutations of these options across the five dimensions (2 304 if the use of a specific date of birth is added to the calculation) that create a fully comprehensive multivariate range of indicators of confidence for age assurance, which gives policymakers, regulators and relying parties the choice to determine the proportionate level of age assurance for any given use-case.

To facilitate interoperability, an existing age check by the previous AA provider needs to be classified against the indicators of confidence defined here. This then allows the AA provider conducting the age check to be confident the previous AA provider has completed a check that meets the standard required in the relying party's age verification practice statement. Using the normative levels of age assurance will increase the opportunities for interoperable re-use of previously completed age checks so is recommended.

A.2 Asserted age

Asserted age is the age claimed by the individual by self-declaration or without the application of age verification components. An asserted age can be captured in a data capture process, by reference to questions asked of the individual or by historical assertion of age.

No attempt is made to validate the claimed age attribute.

No attempt is made to establish the liveness of the individual, nor to prevent false or inaccurate self-declarations being made, nor address any systemic bias in the outcome of the age verification process.

An asserted age is not necessarily an incorrect age but provides a zero level of confidence that the asserted age is the true age.

Although asserted age has unlimited validity over time, it has little value as a source of age verification for future purposes.

NOTE—A policy maker may determine that, an asserted age is unlikely, by itself, to provide sufficient age verification for regulated age-related eligibility decisions, but may be satisfactory for simple, low risk, user experience workflows in applications (such as where the user is merely being asked in what level of detail they would like information to be presented to them). The level of confidence could be increased marginally through technical measures, such as preventing

repeat attempts at entering a date of birth or age, or not guiding the client by preventing the entry of an age which would make them ineligible.

A.3 Indicator of confidence: Accuracy of the outcome levels

Table A.2—Accuracy of outcome levels

Level of confidence	Liveness max false acceptance (failure to acquire)	False positive max (to declared limits)	False negative max (to declared limits)	Upper and lower limits to measure	Accuracy within upper and lower limits	Absolute Limit to measure	Accuracy outside absolute limits	Outcome error parity max
Strict	1%	1%	10%	± 1 years	95%	± 2 years	< 99.95%	1%
Enhanced	1%	1%	10%	± 1 years	95%	± 2 years	< 99.9%	1%
Standard	1%	3%	10%	± 2 years	95%	± 4 years	< 99%	1%
Basic	1%	5%	10%	± 3 years	95%	± 6 years	< 90%	2%

NOTE 1—**liveness false acceptance rate**: The proportion of unauthorized users (i.e., not a genuine, live human being) incorrectly accepted as being live. This only applies to methods of age assurance where there is a risk that a human has been replaced by a fake alternative e.g., facial age estimation.

NOTE 2—**false negative**: An erroneous rejection of the hypothesis that a statistically significant event has been observed. This is also referred to as a type 2 error.

NOTE 3—**false positive**: An erroneous acceptance of the hypothesis that a statistically significant event has been observed. This is also referred to as a type 1 error.

NOTE 4—**outcome error parity** protected groups receiving an equal proportion of positive outcomes, or an equal proportion of errors.

To achieve any given level of assurance, the age assurance process must meet at least each of the applicable minimum requirements for that level. It may exceed the minimum in some dimensions, but the level of assurance achieved is determined by the lowest achievement on any dimension.

It is prudent to assume that with time and resources, most technical solutions can be circumvented. Determining whether a technical solution is sufficient requires an assumption of the threat against which the technical solution seeks to protect. For the purposes of assessing compliance against the levels of assurance in this standard, auditors should assume that attackers have a 1 min of time and US \$10 of resource per attempt to evade the control. If a greater degree of confidence is desired, the auditor may increase the amount of time or resources assumed to be available.

Where age estimation methods are used, the software is often developed to focus on specific ages or age ranges and may be more accurate around these ages than across the full population. For the purposes of assessing compliance against the limits for the levels of confidence in this standard, auditors should generally assume they apply to the variance around the test age for results from test users with a real age that lies within the boundary of the upper and lower limit, and state this in the certification. To fully test a system across all age ranges, then the testing approach shall reflect the distribution of the population.

Auditors shall conduct tests that deliver a statistical level of confidence in the results, and document this level of confidence.

A.3.1 High level of confidence in accuracy of outcome

For age verification systems the following applies:

- No more than 1% of users shall be determined to be more than 1 year older than their actual age when enforcing a minimum age limit (false positives).
- No more than 2% of users shall be determined to be less than 1 year younger than their actual age when enforcing a minimum age limit (false negatives).
- No more than 1% of users shall be determined to be less than 1 year younger than their actual age when enforcing a maximum age limit (false positives).
- No more than 2% of users shall be determined to be more than 1 year older than their actual age when enforcing a maximum age limit (false negatives).

The age estimation systems are as follows:

- 95% of the estimated age of all users shall be determined to be within 1 year of their real age.
- 99.9% of the estimated age of all users shall be determined to be within 2 years of their real age.

The age assurance systems are as follows:

- The process shall include for the liveness of the individual to be established. The failure to acquire rate shall be less than 1%.
- The classification or outcome error parity for protected characteristics for individuals shall not exceed a variance of 1%.

NOTE—High levels of confidence in the accuracy of the outcome of age verification is likely to be useful for policy makers considering very high-risk goods, content, or services; or where seeking to safeguard the health, safety or wellbeing of individuals engaged in making or using very high-risk goods, content, or services.

A.3.2 Medium level of confidence in accuracy of outcome

For age verification systems the following applies:

- No more than 3% of users shall be determined to be more than 1 year older than their actual age when enforcing a minimum age limit (false positives).
- No more than 6% of users shall be determined to be less than 1 year younger than their actual age when enforcing a minimum age limit (false negatives).
- No more than 3% of users shall be determined to be less than 1 year younger than their actual age when enforcing a maximum age limit (false positives).
- No more than 6% of users shall be determined to be more than 1 year older than their actual age when enforcing a maximum age limit (false negatives).

For age estimation systems the following applies:

- 95% of the estimated age of all users shall be within 1 year of their real age.
- 99% of the estimated age of all users shall be within 2 years of their real age.

For all age assurance systems the following applies:

- The process shall include for the liveness of the individual to be established. The failure to acquire rate shall be less than 1%.
- The classification or outcome error parity for protected characteristics for individuals shall not exceed a variance of 1%.

NOTE—A medium level of confidence in the accuracy of the outcome of age verification age verification is likely to be useful for policy makers considering medium-risk goods, content or services; or where seeking to safeguard the health, safety or wellbeing of individuals engaged in making or using medium risk goods, content or services.

A.3.3 Low level of confidence in accuracy of outcome

For age verification systems the following applies:

- No more than 5% of users shall be determined to be more than 1 year older than their actual age when enforcing a minimum age limit (false positives).
- No more than 10% of users shall be determined to be less than 1 year younger than their actual age when enforcing a minimum age limit (false negatives).
- No more than 5% of users shall be determined to be less than 1 year younger than their actual age when enforcing a maximum age limit (false positives).
- No more than 10% of users shall be determined to be more than 1 year older than their actual age when enforcing a maximum age limit (false negatives).

For age estimation systems the following applies:

- 95% of the estimated age of all users must be within 1 year of their real age.
- 95% of the estimated age of all users must be within 2 years of their real age.

For all age assurance systems the following applies:

- The process shall include for the liveness of the individual to be established. The failure to acquire rate shall be less than 1%.
- The classification or outcome error parity for protected characteristics for individuals shall not exceed a variance of 1%.

NOTE—A low level of confidence in the accuracy of the outcome of age verification age verification is likely to be useful for policy makers considering very low-risk goods, content, or services; or where seeking to safeguard the health, safety or wellbeing of individuals engaged in making or using low risk goods, content, or services.

A.4 Indicator of confidence: Frequency of age assurance

In order to maintain the integrity of the age assurance process, it is best practice not to rely on a single check for a lifetime, but to repeat the check periodically, doing so more often for higher-risk use cases. This can help to mitigate the risk of fraudulent checks based on, for example, false documents which might be detected as technology improves over time.

Table A.3—Frequency of age assurance

Frequency of age assurance
Each use
Weekly
Monthly
Annually
Indefinite

A.5 Indicator of confidence: Counter fraud measures

The extent to which an age assurance method counters fraud contributes to the overall level of age assurance. As a minimum, all methods should help to deter false claims. Where contra-indicators are identified, they should be flagged to the relying party. For higher levels of assurance, these contra-indicators should be investigated and resolved, or an alternative form of age assurance used instead.

Table A.4—Counter fraud measures levels

Level of assurance	Deter false claims	Contra-indicators
Resolved	Yes	Resolved or communicated to RP
Communicated	Yes	Unresolved but communicated to RP

A.6 Indicator of confidence: Authentication requirements

Authentication is the process of confirming that the user is the same user who previously completed an age check so that it can be re-used. It is similar to the binding process completed during the age verification process where the evidence used to verify age is checked to confirm it belongs to the user being verified.

Table A.5—Authentication requirements of levels

Level of authentication	Liveness check	Method	Anti-spoofing
3	Yes	User possesses a key through a cryptographic protocol using a “hard” cryptographic authenticator e.g., biometrics with liveness detection	Advanced detection mechanisms design to counter identified risks specific to the use case
2	No	Users must prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required. e.g., authenticator app and PIN	Widely available off-the-shelf detection mechanisms
1	No	Single-factor authentication where the user can prove possession and control of the authenticator through a secure authentication protocol e.g., PIN, Password	Basic system security but no specific anti-spoofing technology
0	N/A	None	None

A.7 Indicators of confidence: Frequency of authentication

It may not always be necessary to authenticate a user for each time age assurance is applied.

Table A.6—Frequency of authentication

Frequency of authentication
Each use
Weekly
Monthly
Annually
Indefinite
NOTE—It is also possible to trigger authentication based on a particular event such as beginning to play an age-restricted game where the age-restriction is higher than the game played previously, or when a headset is transferred to a new user.

A.8 Indicator of confidence: Birth date requirements

Certain regulators may require that a relying party makes use of the user’s actual data of birth as part of the age verification process.

Exactitude may be separately specified to require the use of a specific date of birth in the age assurance process, which may preclude the use of age estimation techniques. This option is for requirements by regulators for the actual date of birth to be considered (although not necessarily retained) as part of an age check. The use of a date of birth in the process does not alone affect the relative reliability of the age check. This option is defined in Table 4.

Table A.7—Birth date requirements for levels

Exactitude requirement	Description
Retained	A specific date of birth is obtained during the age verification process and retained with the user’s record
Included	A specific date of birth is obtained during the age verification process but is not retained after the user’s record has been created at a more general level
Not required	There is no requirement for a date of birth to be part of the age verification process

Annex B

(normative)

Assessing the risk to children: The 4 Cs of online risk

The 4 Cs is a risk framework that classifies risks to children online as content, contact, conduct and contract (sometimes referred to as commercial) risks, or cross-cutting risks for those that fall into more than one category. The framework can be used as a guide to help providers identify different kinds of risks, whether acute or severe, immediate, or cumulative, individual, or multiple.

The examples in the table below include risks from Children Online: Research and Evidence, the ICO's Children's Code Harms Framework, the Australian eSafety Commissioner's Safety by Design work and the OECD's Revised Typology of Risks for children in the digital environment. They are indicative of the types of risks children may be exposed to online. The lists are not exhaustive, but they give a good indication of the breadth of risks that should be considered. Organizations should record and address any other risks they uncover during the process of assessing risk.

Content risks	Contact risks	Conduct risks	Contract risks (or commercial)
A child or young person experiences content risks when they are exposed to harmful material. They include:	Contact risks arise when a child or young person participates in an activity with a malign actor, often, but not always, an adult. They include:	A child or young person encounters conduct risks when they are involved in an exchange, often, but not always, peer-to-peer, as either a perpetrator, victim, or sometimes both. They include:	Contract or commercial risks occur when a child or young person is exposed to inappropriate commercial contractual relationships or pressures. They include:
<ul style="list-style-type: none"> Violent material Child sexual abuse material (CSAM) Developmentally inappropriate content Extremism Eating disorder promotion Disinformation/misinformation Scams Body image pressures 	<ul style="list-style-type: none"> Child sexual exploitation and abuse (CSEA), including grooming Developmentally inappropriate activity Catfishing (targeting a victim by using a fake identity) Scams blackmail Stalking, unwanted surveillance 	<ul style="list-style-type: none"> Trolling Cumulative or volumetric attacks ('pile-ons') Sexual extortion ('sextortion') Non-consensual sharing of intimate material or image-based abuse Bullying, abuse, insults, rumors, social exclusion Individual identity attacks Dehumanization Hate speech Sexual harassment/aggression Doxing (publishing private information) Extremism Direct and indirect threats of violence, intimidation and harassment Doctored images (including deepfakes and shallow fakes) Scams Stalking, unwanted surveillance Chilling effects on free expression Over-exposure, over-sharing 	<ul style="list-style-type: none"> Loss of digital footprint Hidden costs Compulsive use Identity theft Fraud phishing scams Gambling Inaccurate profiling Bias in automated decision-making Excessive data collection and sharing
Cross-cutting risks	A number of risks to children online cut across some or all of the categories of risk, and result in children being exposed to infringements of their privacy, threats to their health or unfair treatment. Cross-cutting risks include:	—	—
<ul style="list-style-type: none"> Infringement of privacy Adverse effect on data rights Restriction of access to services 	<ul style="list-style-type: none"> Discrimination Risks to physical and mental health 	<ul style="list-style-type: none"> Interference with sleep or schoolwork Security risks Parental surveillance 	<ul style="list-style-type: none"> Addiction, compulsive use Loss of non-financial resources (e.g., time, sleep)

B.1 Risk profiles

Regulators around the world are considering developing risk profiles of online services, with greater oversight of those deemed to pose greater risks to children, taking into account the features and impact of a service rather than its size. Small does not mean safe. A service with a smaller number of users can still cause significant harm and a company with a small turnover or workforce can still reach a vast number of users. As in many other sectors, designing safe products and services is simply the price of doing business for any trading company. Smaller providers need support to comply, not permission to harm.

B.2 Risk register of common features

Providers should assess the risks presented by each feature of the product or service to reveal known harms, potential risks, and unintended consequences. The table below sets out common features of services children use. Providers should use the table to consider the potential for their own features to negatively impact children, with attention paid to how certain features might impact different groups of children. At the end of this process, providers will be able to identify elements or features that may need to be disabled, redesigned, or carry warnings and/or other mitigation measures in order to keep children safe. It will also allow providers to make positive changes that deliver enhanced, creative, and age-appropriate experiences.

Providers should consider both the likelihood of harm occurring and the severity of harm when it does occur. The likelihood of a child encountering harm can be measured by, among other methods, peer-reviewed academic research, internal research, A/B testing and data from public bodies. Providers should make use of child development experts, official advice from public health authorities and the testimony of children themselves when measuring the severity of harm.

For more information on how the design of features can contribute to risk to children, and how and when the same features can impact children differently depending on their individual characteristics and circumstances, see Ofcom’s report, *Research into risk factors that may lead children to harm online*.

Table B.1—Risk register of common features

Features	Risk category	Potential harms	Likelihood of harm	Severity of harm
Friend recommendations that introduce adults to children	Contact, Conduct	Child sexual exploitation and abuse (CSEA) Developmentally inappropriate activity Phishing and catfishing		
Notifications on by default	Conduct, Contract	Loss of non-financial resources (e.g., time, sleep) Unwarranted intrusion		
Discoverable location	Contact, Conduct, Contract	Bodily harm Unwarranted intrusion		
Targeted advertising on by default	Content, Contract	Unwarranted intrusion Undue commercial pressure Financial harm Manipulation and exploitation		
Lootboxes	Contract	Hidden costs Compulsive use Gambling		

Table continues

Table B.1—Risk register of common features (continued)

Features	Risk category	Potential harms	Likelihood of harm	Severity of harm
In-service ‘gifts’	Contract	Child sexual exploitation and abuse (CSEA) Developmentally inappropriate activity Catfishing Scams		
End-to-end encryption	Content, Contact	Child sexual abuse material (CSAM) Developmentally inappropriate content Extremism Child Sexual Exploitation and Abuse (CSEA) Developmentally inappropriate activity		
Low-privacy profiles by default	Contact	Child sexual exploitation and abuse (CSEA) Stalking, unwanted surveillance Identity theft Catfishing		
Direct messaging of children by unknown adults	Contact	Child sexual exploitation and abuse (CSEA) Developmentally inappropriate activity Catfishing Stalking, unwanted surveillance		
Livestreaming/ video chat	Contact, Conduct	Child sexual exploitation and abuse (CSEA) Developmentally inappropriate activity Blackmail Stalking, unwanted surveillance Over-exposure, over-sharing		
Video-sharing	Content, Conduct	Child sexual exploitation and abuse (CSEA) Developmentally inappropriate activity Blackmail Stalking, unwanted surveillance Over-exposure, over-sharing		
Image-sharing	Content, Conduct	Stalking, unwanted surveillance Over-exposure, over-sharing Body image pressures		
Anonymity	Contact, Conduct	Child sexual exploitation and abuse (CSEA) Catfishing Stalking, unwanted surveillance Trolling Bullying, abuse, insults, rumors, social exclusion		
Search functions	Content, Contract	Violent material Developmentally inappropriate content Eating disorder promotion Disinformation/misinformation		

Table continues

Table B.1—Risk register of common features (continued)

Features	Risk category	Potential harms	Likelihood of harm	Severity of harm
Engagement ‘streaks’	Contract	Addiction, compulsive use Over-exposure, over-sharing Excessive data collection		
Algorithmic curation of feeds	Content, Contract	Violent material Developmentally inappropriate content Extremism Eating disorder promotion Disinformation/misinformation Scams Body image pressures Inaccurate profiling Bias in automated decision-making Excessive data collection, sharing		
Virality	Content, Conduct	Developmentally inappropriate content Body image pressures Developmentally inappropriate activity Over-exposure, over-sharing		
Endless scroll	Content Contract	Compulsive use Loss of non-financial resources (e.g., time, sleep)		
Popularity metrics	Contact, Conduct	Child sexual exploitation and abuse (CSEA), including grooming Developmentally inappropriate activity Stalking, unwanted surveillance Over-exposure, over-sharing		
Autoplay	Content, Contract	Addiction, compulsive use		
Trending lists	Content, Conduct	Developmentally inappropriate content Disinformation/misinformation Addiction, compulsive use		
Disappearing/ time-limited content	Content, Contract	Violent material Child sexual abuse material (CSAM) Developmentally inappropriate content Extremism Scams Addiction, compulsive use		

Table continues

Table B.1—Risk register of common features (continued)

Features	Risk category	Potential harms	Likelihood of harm	Severity of harm
Disappearing/time-limited messages	Content, Contact	Child sexual exploitation and abuse (CSEA) Developmentally inappropriate activity Scams Blackmail Sexual extortion ('sextortion') Non-consensual sharing of intimate material or image-based abuse Bullying, abuse, insults, rumors, social exclusion Direct and indirect threats of violence, intimidation and harassment Doctored images (including deepfakes and shallow fakes)		
Groups	Content, Contact, Conduct	Violent material, Child Sexual Abuse Material (CSAM) Developmentally inappropriate content Extremism Eating disorder promotion Disinformation/misinformation Developmentally inappropriate activity Hate speech Chilling effects on free expression Over-exposure, over-sharing		
Pay-to-play	Contract	Hidden costs Restriction of access to services		
Autocomplete	Content, Contract	Developmentally inappropriate content Inaccurate profiling		
People also liked...	Content, Contract	Developmentally inappropriate content Disinformation/misinformation Inaccurate profiling		
Image altering (filters)	Conduct	Body image pressures Doctored images (including deepfakes and shallow fakes)		
'Creator' accounts	Content, Conduct, Contract	Over-exposure, over-sharing Undue commercial pressure		

Annex C

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] 5Rights Foundation 5Rights Framework.¹⁴

[B2] ISO/IEC 25063.3, Systems and software engineering—Systems and software product Quality Requirements and Evaluation (SQuaRE)—Common Industry Format (CIF) for usability: Context to use description.¹⁵

[B3] UK Information Commissioner’s Office, Introduction to the Age-appropriate design code.¹⁶

[B4] United Nations Committee on the Rights of the Child General Comment (15), 2013 on The Right of the Child to the Enjoyment of the Highest Attainable Standard of Health.¹⁷

[B5] United Nations Committee on the Rights of the Child General Comment (16) on State Obligations Regarding the Impact of Business on Children’s Rights.¹⁸

[B6] United Nations Department of Economic and Social Affairs, Transforming Our World: the 2030 Agenda for Sustainable Development.¹⁹

[B7] United Nations Guiding Principles of Business and Human Rights.²⁰

[B8] United Nations Millennium Declaration.²¹

[B9] United Nations Principles for Responsible Management Education. The Six Principles for Responsible Management Education.²²

[B10] United Nations Sustainable Development Goals: A Guide for Business and Management Education.²³

¹⁴Available at: <https://5rightsfoundation.com/about-us/the-5-rights/>.

¹⁵ISO publications are available from the International Organization for Standardization (<https://www.iso.org/>) and the American National Standards Institute (<https://www.ansi.org/>).

¹⁶Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.

¹⁷Available at: <https://www2.ohchr.org/english/bodies/crc/docs/GC/CRC-C-GC-15-en.doc>.

¹⁸Available at: <https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.16.pdf>.

¹⁹Available at: <https://sdgs.un.org/2030agenda>.

²⁰Available at: <http://sol.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHREN.pdf>.

²¹Available at: <https://sol.ohchr.org/EN/ProfessionalInterest/Pages/Millennium.aspx>.






²²Available at: <https://www.unprme.org/>.

²³Available at: <https://sol.un.org/sustainabledevelopment/sustainable-development-goals>.



RAISING THE WORLD'S STANDARDS

Connect with us on:

-  **Twitter:** twitter.com/ieeesa
-  **Facebook:** facebook.com/ieeesa
-  **LinkedIn:** linkedin.com/groups/1791118
-  **Beyond Standards blog:** beyondstandards.ieee.org
-  **YouTube:** youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060