Age Appropriate
Design Certification Scheme

Technical Requirements for Age Appropriate Design for Information Society Services

ACCS 3: 2021



Age Check Certification Services Ltd
UKAS PRODUCT CERTIFICATION 21037

© Age Check Certification Scheme Ltd (2021) All Rights Reserved



This is a publicly available specification created by the Age Check Certification Scheme Ltd. It is subject to the intellectual property rights of the Scheme and may not be copied, used in a retrieval system or utilised without the express consent of the Scheme, save that it may be mentioned by name as a reference document with appropriate attribution and a link to the document itself.
© Age Check Certification Scheme Ltd 2021. All rights reserved.

The certification criteria contained within this document have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK General Data Protection Regulation.





Content

Introduction 4

1. Scope 7

- Scope of Scheme Criteria for Information Society Services 8
- Types of Information Society Services in Scope 8
- Types of Information Society Services Not in Scope 9
- Types of Data Processing by Information Society Services in Scope 10
- Processing by Information Society Services Not In Scope 11
- Target of Evaluation for Information Society Services 12
- Territorial Scope 13

2. Normative References 15

- Age Check Certification Scheme 16
- Legal Provisions 16
- National and International Standards 17
- Other Documents 17

3. Terms and Definitions 19

4. Technical Requirements for Data Protection and Privacy 25

- Leadership and Oversight of Data Protection Responsibilities 26
- Data Protection Management Systems 27
- Information Security and Risk Management 27
- Data Protection Personnel and Training 28
- General Data Processing Requirements 28

5. Requirements for Age Appropriate Design 31

- Best Interests of the Child 32
- Data Protection Impact Assessments 32
- Age Appropriate Application 36
- Transparency 38
- Detrimental Use of Data 41
- Policies and Community Standards 43
- Default Settings 43
- Data Minimisation 45

Data Sharing 45
Geolocation 46
Parental Controls 46
Profiling 47
Nudge Techniques 51
Connected Toys and Devices 52
Online Tools 54

Introduction

The Age Check Certification Scheme tests that age check systems work. These can be an integral part of information society services that may be intended for or accessed by children; or may be specifically intended only for use by adults. As an extension of this work, the Scheme can also assess conformity with technical requirements for age appropriate design for online services.

Under s.123 of the Data Protection Act 2018, the UK Information Commissioner has published a Code of Practice for the Age Appropriate Design of Information Society Services. This is sometimes known as the **Children's Code** and will be referred to as '**the Code**' within this document. It is rooted in the United Nations Convention on the Rights of the Child (UNCRC) that recognises the special safeguards children need in all aspects of their life, including General Comment 25 on the Digital Rights for Children. Data protection law in the UK reflects this and provides its own additional safeguards for children.

The Code, and this Certification Scheme supporting it, is the first of its kind, but it reflects the global direction of travel with similar reform being considered in the USA, Europe and globally by the Organisation for Economic Co-operation and Development (OECD).

These technical requirements only cover data processing **in the context of** the application of the Children's Code to the data processing of information society services to demonstrate conformity with the Code. They do not cover the broader data processing activities of Scheme Clients.

The Scheme is operated through our UKAS accredited conformity assessment body (Age Check Certification Services Ltd) and the certification criteria contained within this document have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK GDPR.

The Scheme has set out ACCS 2:2021 – Technical Requirements for Data Protection and Privacy, which apply **in addition to** the technical requirements set out in this document insofar as they apply to the context of application of the Code to the Scheme Client's data processing. To avoid unnecessary duplication, sections of these technical requirements cross reference with ACCS 2:2021 where appropriate.

This document defines the technical, organisational and documentary requirements that information society services in scope need to demonstrate to conform with the requirements of the Code. The requirements are set out in 15 sections of these technical requirements, that align with the Code:

a) **Best Interests of the Child:** The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child

b) **Data Protection Impact Assessments:** Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this Code

c) **Age Appropriate Application:** Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this Code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this Code to all your users instead

d) **Transparency:** The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated

e) **Detrimental Use of Data:** Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice

f) **Policies and Community Standards:** Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies)

g) **Default Settings:** Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child)

h) **Data Minimisation:** Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate

i) **Data Sharing:** Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child

j) **Geolocation:** Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session

k) **Parental Controls:** If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored

l) **Profiling:** Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing)

m) **Nudge Techniques:** Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections

n) **Connected Toys and Devices:** If you provide a connected toy or device, ensure you include effective tools to enable conformance to this Code

o) **Online Tools:** Provide prominent and accessible tools to help children exercise their data protection rights and report concerns

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguarding concerns and their rights in relation to the processing of personal data. Any information given to, or provided in communication with, a child shall be in such a clear and plain language that the child can easily understand. Where a child asks a business to provide a service for which payment is normally made and processes data on the basis of consent, parental consent may be required unless the child is aged 13 years or over. These technical requirements recognise that organisations carrying out age assessments and providing information society services have particular responsibilities when handling the personal data of a child.

Any certification against the Age Check Certification Scheme does not reduce the responsibility of the data controller or the data processor to comply with UK GDPR and is without prejudice to the tasks and powers of the ICO. However, gaining independent 3rd party certification from an ICO approved certification scheme can help you demonstrate your conformance to the Code if they ask you to do so. You can do this by providing a copy of your Certificate of Conformity. We also notify the ICO that a Certificate of Conformity has been issued to you and the ICO will take this into account as part of any subsequent investigation.

The Age Check Certification Scheme Rules and these technical requirements have been designed to comply with ISO/IEC 17065:2012, the Information Commissioner's UK additional accreditation requirements for certification bodies, the relevant regulatory requirements for age verification service providers, the provisions of UK GDPR, the appropriate product and service standards and the requirements of the Trade Mark Rules 2008.

[1]Article 8 of UK GDPR restricts the processing of children's data where the lawful basis of consent is used to require the consent of a holder of parental responsibility over the child where the child is under 16 years of age. However, UK GDPR amends that (as is permitted by UK GDPR) to be 13 years of age.

1

Scope

Scope



1. Scope

1.1 The suite of Age Check Certification Scheme (ACCS) Standards (described in Section 2 – Normative References) are applicable to Scheme Clients submitting their products, processes or services for certification from ACCS and who wish to have access to use of the ACCS certification mark as a mark of conformity. These technical requirements specifically cover the processing of personal data within those products, processes or services as the object of the UK GDPR certification in the context of applying the Age Appropriate Design Code to the Scheme Client's data processing.

PLEASE NOTE: These technical requirements do not cover all of the data processing operations of information society services. They only cover the application of the Age Appropriate Design Code to their data processing and how the Scheme Clients have addressed the implications of the Code on decisions made, policies generated, information published and securing the data rights of children in the context of acting in the best interests of the child.

Scope of Scheme Criteria for Information Society Services

1.2 These technical requirements apply to the data processing operations of any information society services likely to be accessed by children in the UK. This includes many apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet. It is not restricted to services specifically directed at children.

Types of Information Society Services in Scope

1.3 These technical requirements apply to any Scheme Client that processes data for services likely to be accessed by children including:

a) coding and functionality of apps, programs and websites including search engines

b) providing social media platforms, online messaging, chat or user generated content

c) provision of internet based voice telephony services

d) online marketplace

e) provision of content streaming services (e.g. video, music or gaming services) including Audio Visual Media Services

f) online games

g) news or educational websites (but note some significant exemptions applicable to these services)

h) any websites offering other goods or services to users over the internet

i) the provision of electronic services for controlling connected toys and other connected devices

1.4 If the service is designed for and aimed specifically at under-18s then these technical requirements apply. However, the provision in section 123 of the DPA is wider than this. It also applies to services that are not specifically aimed or targeted at children, but are nonetheless likely to be used by under-18s and are therefore within the scope of these technical requirements.

1.5 In practice, whether the information society service is likely to be accessed by children or not is likely to depend on:

a) the nature and content of the service and whether that has particular appeal for children

b) the way in which the service is accessed and any measures that are put in place to prevent children gaining access, such as the application of age assurance or age verification systems.

1.6 If the information society service is not aimed at children but is not inappropriate for them to use either, then the focus should be on assessing how appealing the service can be to them. If the nature, content or presentation of the service is such that children want to use it, then these technical requirements apply.

Types of Information Society Services Not in Scope

1.7 The following types of information society services are not in scope for this certification scheme (or the Code):

a) a public authority providing online public services on a non-commercial basis

b) a police force or other competent authority processing personal data for law enforcement purposes

c) a provider of a website that just provides information about their real-world business, but does not allow customers to buy products online or access a specific online service

d) a provider of an online booking service for an in-person appointment

e) a provider of voice telephony services unless they are internet based voice calling services (VOIP)

f) a provider of scheduled television or radio transmissions that are broadcast to a general audience, rather than at the request of the individual – called 'on-demand' services (even if the channel is broadcast over the internet)

g) a provider of online counselling or other preventative services (such as health screenings or check-ups) to children

Types of Data Processing by Information Society Services in Scope

1.8 Scheme Clients providing information society services likely to be accessed by children may be undertaking one or more of the following types of data processing (this is not an exhaustive list):

a) **Data Acquisition:** including the process of gathering data from users about their usage of the information society service

b) **Customer and User Records:** enabling account creation, user authentication and identification (including facial recognition or fingerprint data)

c) **Authentication Tokens:** the provision of data packets that provide a user with ongoing authentication records (such as cookies)

d) **Demographic Data:** enabling monitoring, targeting and tailoring of services to different demographics or audience segmentation (including age groups, socio-economic or cultural backgrounds)

e) **Age Attributes:** gathering of claimed age attributes and verification of these against a reliable source of authentication, perhaps through certified Age Check processes described in ACCS 4 – Technical Requirements for Age Check Services

f) **Consent, Including 3rd Party Parental or Guardianship Consent:** including any processing of data indicating agreement to the processing of personal data relating to him or her or their child or a child that they exercise parental responsibility for

g) **Personal Identifiable Information:** gathering of data from users about their personal identity, behaviours and history

h) **User Generated Content:** including images, videos, media files, articles, 'posts', chat and interactive content

i) **Data Storage:** including location of servers, centralised or de-centralised storage, encryption and retention/accessibility

j) **Technical Data Processing:** such as cyber security measures, physical security, systems protection and information systems management systems

k) **Commoditisation of Data:** such as providing data to organisations (whether for a fee or not) for the purpose of facilitating advertising, supplying content or services, algorithmic driven services or communications to children

l) **Interoperability Systems:** such as connected toys and devices, inter-game interoperability, cross-platform data sharing, metadata and structured datasets (such as those established to support data portability)

m) **Profiling:** including automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to behaviours of children such as tracking online activity, behaviours, interests, opinions and beliefs

n) **Biometric Data:** including processing of biometric or inherent features for identification, health records, movement and capability (such as cognitive skill) data

o) **Compliance Data:** including monitoring, moderating or implementing compliance with policies and community standards, industry codes of practice or legal obligations

p) **Geolocation Data:** including the ability to track, monitor and share historical movement, current location or predict future movement of children

q) **Relationship Data:** including relationships with parents, guardians, relatives, other children or other users of the information society service (including intimate or close relationships)

r) **Special Category Data:** including origins, political views, religious or philosophical beliefs, genetic information, health data, biometrics, sex life (including specifically children exploring their sexual orientation, behaviours and beliefs) and involvement in criminal activity or similar security measures

s) **Mental Health Data:** including current or past mood, outlook, aspirations, intent and specifically monitoring for suicide or self-harm

t) **Enabling Data Rights:** including services that support children exercising their data rights or working with parents or guardians to support asserting data rights on behalf of the child

u) **International data processing:** where targets of evaluation utilise data resources from outside of the United Kingdom

Processing by Information Society Services Not In Scope

1.9 These technical requirements do not apply to the processing of any personal data that does not take place in the context of the Scheme Client's approach to implementation of the Age Appropriate Design Code.

1.10 The types of data processing not in scope include (but are not limited to):

a) **Adult Services:** including any services exclusively provided for the use of or enjoyment by adults (and where appropriate age verification is in place)

b) **Public Services:** including the processing of data by any public body on a non-commercial basis for the purpose of providing public services to or on behalf of children

c) **Internal Employee Records:** including the processing of data about individual employees, contractors or service providers to the Scheme Client

d) **Commercial Relationships:** including the processing of data to facilitate the arrangements between corporate entities in a supply chain or service fulfilment (save to the extent that such data processing affects the data rights of children)

e) **Elections:** including the processing of data relating to any election for public office where an elector is required by law to be over 18

Target of Evaluation for Information Society Services

1.11 The Target of Evaluation is all processing of personal data by the Scheme Client's information society service likely to be used by children.

1.12 The Scheme Client shall define the targeted processing operations concerned with the delivery of their information society service and describe them in terms of:

a) data types, systems and processes used

b) where the processing subject to evaluation starts and ends

c) any interfaces and interdependent processing operations

d) all relevant processing operations, illustration of data flows

e) any processing on shared or externally hosted systems or by data processors acting on behalf of the Scheme Client

f) a determination of the Target of Evaluation's area of application

g) any special types of processing e.g. automated decision making, profiling, high risk processing

1.13 The Scheme Client shall define any processing operations that are outside the scope of the certification and provide an explanation as to why they have included or excluded certain aspects of their processing.

1.14 An accurate specification of the Target of Evaluation is of fundamental importance for the certification procedure as it decides on what is covered by the certification.

1.15 The Target of Evaluation shall be described on the Certification Documentation.

1.16 The relevant scope set out above shall be determined for each information society service submitted for evaluation as a part of the application review process.

1.17 The relevant scope shall include the identification of any special category data (such as inherent or biometric features) or any processing of data for automated decision making.

Territorial Scope

1.18 These technical requirements apply to any information society services:

a) that are established in the United Kingdom

b) that are established outside of the United Kingdom but either:

a. offer goods or services (even if for free) to individuals in the United Kingdom or

b. monitor the behaviour of individuals in the United Kingdom

1.19 Scheme Clients that are non-UK organisations shall appoint a UK representative, with a mandate of authority to act on behalf of the Scheme Client in the UK. The UK representative may be an individual, or a company or organisation established in the UK, and shall be able to represent the Scheme Client regarding their obligations under the UK GDPR (e.g. a law firm, consultancy or private company).





2

Normative References

Normative References



2. Normative References

Age Check Certification Scheme

The Age Check Certification Scheme is built on a modular approach to applicable standards and technical requirements. As a part of the Application Review Process, a Certification Officer assesses the applicable requirements for the business model of the Scheme Client. The suite of applicable requirements is constantly changing as new methodologies emerge, new standards are developed and new technical requirements are introduced. A full comprehensive current list can be found on the Standards Section of the Scheme website, but include:

ACCS 0: 2021 – General Scheme Rules (covering the process of certification under ISO 17065:2012)

ACCS 1: 2020 – Technical Requirements for Age Estimation Technologies

ACCS 2: 2021 – Technical Requirements for Data Protection and Privacy*

ACCS 3: 2021 – Technical Requirements for Age Appropriate Design for Information Society Services*

ACCS 4: 2020 – Technical Requirements for Age Check Providers

ACCS 5: 2021 – Technical Requirements for Age Check System Penetration Testing and Vulnerability Scans; (In Development)

ACCS 6: 2021 – Technical Requirements for Parental Consent or Social Proofing for Age Gateway Technologies. (In Development)

* **ACCS 2:2021** and **ACCS 3:2021** are technical requirements that have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK GDPR

Legal Provisions

The principal legal provisions relevant to data processing by information society services are:

- Communications Act 2003 as amended by various Audio Visual Media Services Regulations
- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679 as it applies in the United Kingdom by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 as amended
- Privacy and Electronic Communications Regulations 2003 (PECR)

National and International Standards

ISO 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services.

Scheme Clients should be aware that there are a series of emerging international and national standards relating to age appropriate design, which may be of use in preparation for audit. Once adopted, these may be referred to in future options for these technical requirements.

Other Documents

Scheme Clients will find a substantial amount of supporting materials, guidance, advice and templates to assist with preparing and implementing their data protection systems. This section provides a list of some of the relevant materials that have been used in the preparation of this scheme or may be useful to Scheme Clients.

Advertising Codes – from the Advertising Standards Authority – https://www.asa.org.uk/codes-and-rulings/advertising-codes.html

Age Appropriate Design Code – https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

BGC Code of Conduct – https://bettingandgamingcouncil.com/uploads/Downloads/BGC-CODE-OF-CONDUCT.pdf

BGC Code for Game Design – https://bettingandgamingcouncil.com/uploads/Downloads/8-V2-IGRG-GAMBLING-INDUSTRY-CODE-FOR-SOCIALLY-RESPONSIBLE-ADVERTISING-21.4.21.pdf

BGC Code for Socially Responsible Gambling Advertising – https://bettingandgamingcouncil.com/uploads/Downloads/BGC-GAMBLING-INDUSTRY-CODE-FOR-SOCIALLY-RESPONSIBLE-ADVERTISING.pdf

Portman Group Codes of Practice – https://www.portmangroup.org.uk/codes-of-practice/

UK code of practice for the self-regulation of new forms of content on mobiles – https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/ukcode

The use of guidance and materials published by the UK Government or the Information Commissioner's Office is under terms of the licence under the **Open Government Licence** (OGL) v3.0. – *http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/*





Terms and Definitions



3. Terms and Definitions

In this document:

"shall" indicates a requirement

"should" indicates a recommendation

"may" indicates a permission

"can" indicates a possibility or a capability

GUIDANCE NOTES are shown in italic text and are intended to assist the reader with understanding provisions.

When referring to the ACCS Standards, refer to the ACCS Standard, followed by the year of issue, followed by the provision – such as **ACCS 0:2021, 4.3.**

3.1 Age Appropriate Design Code (AADC)	means the Code of Practice laid before Parliament and issued under s.123 of the Data Protection Act 2018.
3.2 Age Assurance	means the process of gaining a reliable indication of the age of an individual to an appropriate level of confidence.
3.3 Age Check Practice Statement	means the document describing the operational practices and procedures of an age check service [PAS 1296:2018 – 2.1.1].
3.4 Age Estimation	means an indication by estimation that a citizen is likely to fall within a category of ages, over a certain age or under a certain age to a specified level of confidence by reference to inherent features or behaviours related to that citizen.
3.5 At a distance	means that the information society service is provided without the parties being simultaneously present.
3.6 Best interests of the child	means that in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration [Article 3 of the United Nations Convention on the Rights of the Child (UNCRC)].
3.7 Certification Requirement	means a specified requirement that is fulfilled by the client as a condition of establishing and maintaining certification [ISO 17065:2012 – 3.7].
3.8 Certification Scheme	means the Age Check Certification Scheme [ISO 17065:2012 – 3.9].

3.9 Client	means an organisation that has applied to the Scheme Conformity Assessment Body, Age Check Certification Services Ltd, for certification or been granted certification that is responsible to ACCS for ensuring that the certification requirements are fulfilled [ISO 17065:2012 – 3.1].
3.10 Consent	means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
3.11 Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.
3.12 Data Protection by Design and Default	means the appropriate technical and organisational measures as required by Article 25 of UK GDPR.
3.13 Data Sharing Code	means the Code of Practice laid before Parliament and issued under s.121 of the Data Protection Act 2018.
3.14 Electronic means	means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means.
3.15 Evaluation	means the combination of the selection and determination functions of conformity assessment activities against the scheme rules [ISO 17065:2012 – 3.3].
3.16 Geolocation	means data taken from a user's device which indicates the geographical location of that device, including GPS data or data about connection with local Wi-Fi equipment.

3.17 High Risk Processing	means high risk processing can include the processing of: • special category data; • personal data of vulnerable natural persons, in particular of children; • personal aspects evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; • processing involving a large amount of personal data and affecting many data subjects.
3.18 ICO	means Information Commissioner's Office.
3.19 Individual Request	means 'at the individual request of a recipient of services' which means that the service is provided through the transmission of data on individual request.
3.20 Information Society Service	means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
3.21 Personal Data	means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
3.22 Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
3.23 Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3.24 Recipient	means a natural or legal person, public authority, agency or another body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with UK law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
3.25 Remuneration	means for money or money's worth and includes where the funding of the service does not come directly from the end user. ***Note:*** *For example, an online gaming app or search engine that is provided free to the end user but funded via advertising still comes within the definition of an Information Society Service. These requirements also cover not-for-profit apps, games and educational sites, as long as those services can be considered as 'economic activity' in a more general sense. For example, they are types of services which are typically provided on a commercial basis.*
3.26 Scheme Owner	means the Age Check Certification Scheme Ltd [ISO 17065:2012 –3.11].
3.27 Top Management	means a person or group of people who directs and controls an organisation at the highest level.
3.28 UKAS	means United Kingdom Accreditation Service.
3.29 UNCRC	means United Nations Convention on the Rights of the Child.
3.30 UK GDPR	means General Data Protection Regulation (EU) 2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and section 205(4) of the Data Protection Act 2018.





4

Technical Requirements for Data Protection and Privacy



4.Technical Requirements for Data Protection and Privacy

4.1 These technical requirements cover the implementation of the Code, but there are additional technical requirements for Data Protection and Privacy as set out in ACCS 2:2021 and applied as set out in this section for all Scheme Clients for certification of Age Appropriate Design of Information Society Services.

> ***Note 1:*** *In some cases, the context of the requirements in ACCS 2:2021 relate more specifically to age check providers and other clients under the Scheme. These will need to be interpreted as appropriate for the context of age appropriate design.*
>
> ***Note 2:*** *To avoid unnecessary duplication in this document, the following requirements are set out in ACCS 2:2021.*

Leadership and Oversight of Data Protection Responsibilities

4.2 Top Management of Scheme Clients shall:

a) make and publish an Age Appropriate Design Policy Statement setting out a commitment to securing the best interests of the child in the Scheme Client's approach to the provision of its information society services

b) on a regular basis (as a minimum annually) consider, approve, update and record its Data Protection Management System (as set out in ACCS 2; s.4.1.2) in the context of implementation of the Code

c) be accountable for decisions made about data protection (as set out in ACCS 2; s.4.1.3 and further as set out in s. 4.4 below)

d) maintain an open and honest approach to data processing (as set out in ACCS 2; s.4.1.3)

e) comply with all transparency obligations (as set out in ACCS 2; s.4.1.3)

f) be responsible for ensuring that the Scheme Client have determined and documented the lawful basis of processing data for their information society service prior to commencing any processing of that data (as set out in ACCS 2; s.4.1.4)

> ***Note 1:*** *In addition to the general requirements about accountability set out in ACCS 2:2021, Scheme Clients shall implement an accountability programme to effectively address the standards in these technical requirements and the Code. This can be tailored to the size and resources of the Scheme Client and the risks to children inherent in the online service.*

4.3 The Accountability Programme shall be driven by the Data Protection Officer, if one has been appointed, and overseen by senior management at Board level if the Scheme Client is structured in this way. For smaller businesses which may not have such formal structures, it is still important to make sure that children's privacy is understood by key personnel and is seen as an important business priority and key accountability measure.

4.4 Scheme Clients shall assess and revise the Accountability Programme on an ongoing basis, building in changes to reflect the changing environment of children's privacy.

4.5 Scheme Clients shall report against these technical requirements in any internal or external accountability reports, introducing KPIs (key performance indicators) on children's privacy to support this as appropriate.

> ***Note 1:*** *Scheme Clients may find the Information Commissioner's Accountability Framework a useful guide for implementing appropriate requirements under this section.*

Data Protection Management Systems

4.6 Scheme Clients shall establish, document, implement and maintain appropriate data protection policies which state its commitment to deliver information society services likely to be accessed by children and involving personal data processing in compliance with UK GDPR, the Children's Code and its requirements in relation to these technical requirements.

4.7 The minimum requirements for data protection management systems are set out in:

a) **ACCS 2; s.4.3.3** (content of data protection management system)

b) **ACCS 2; s.4.3.4** (management of documented information)

c) **ACCS 2, s.4.3.5 – s.4.3.7** (records of processing activities)

d) **ACCS 2; s.4.3.8 – s.4.3.9** (data retention policies)

e) **ACCS 2; s.4.3.10 – s.4.3.13** (internal audit)

> ***Note 1:*** *References in the sections of ACCS 2 listed above to the 'Target of Evaluation' should be read as references to the 'Target of Evaluation' in ss. 1.11 – 1.17 of these technical requirements.*

Information Security and Risk Management

4.8 Scheme Clients shall establish, implement, maintain and continually improve a set of policies and procedures (Information Security Management System), which ensure the confidentiality, integrity and availability of systems and services, including the physical and cyber security of data covering the whole life cycle of the data in the context of providing information society services likely to be accessed by children.

4.9 The minimum requirements for information security and risk management are set out in:

a) **ACCS 2; s.4.4.2** (security of personal data)

b) **ACCS 2; s.4.4.3 & s.4.4.5** (risk assessment)

c) **ACCS 2; s.4.4.4** (security measures)

d) **ACCS 2; s.4.4.6** (cyber security)

e) **ACCS 2; s.4.4.7** (annual review)

f) **ACCS 2; s.4.4.8** (access restoration)

g) **ACCS 2; s.4.4.9** (intervening in data processing)

h) **ACCS 2; s.4.4.10** (encryption)

i) **ACCS 2; s.4.4.11** (penetration testing)

4.10 In considering the publication about any aspects of the Information Security Management System for users, particularly for children, Scheme Clients shall comply with the requirements for age appropriate transparency set out in s.5.4 of these technical requirements.

Data Protection Personnel and Training

4.11 Scheme Clients shall:

a) appoint a Data Protection Officer and assign the responsibilities for that Officer as set out in the requirements in ACCS 2; s.4.5

b) if a Data Protection Officer is not required by ACCS 2; s.4.5, appoint a person of sufficient seniority to provide advice on data protection and age appropriate design matters

c) implement a programme of training and education for personnel having access to personal data as set out in the requirements in ACCS 2; s.4.7

d) take responsibility for and manage the activities of any sub-contractors or sub-processors as set out in the requirements in ACCS 2; s.4.8

General Data Processing Requirements

4.12 Scheme Clients shall:

a) establish their lawful basis of processing, including the fairness of processing, taking into account the best interests of the child, in accordance with ACCS 2; s.5.2

b) have clearly identified the purpose or purposes for processing personal data, taking into account the best interests of the child, in accordance with ACCS 2; s.5.3

c) only collect personal data that they actually need for their specified purposes, taking into account the best interests of the child, in accordance with ACCS 2; s.5.4 and with particular reference to s.5.8 of these technical requirements

d) ensure that any personal data created by their processing is accurate and kept up to date, taking into account the best interests of the child, in accordance with ACCS 2; s.5.5

e) limit the use and storage of data in line with their own documented retention policies and retention schedules, taking into account the best interests of the child, in accordance with ACCS 2; s.5.6

f) respect general data subject rights, making particular allowance for the data subject potentially being a child, or having a person exercising data subject rights on behalf of a child, in accordance with ACCS 2; s.5.7 and with particular reference to s.5.15 of these technical requirements

g) handle special category data in accordance with ACCS 2; s.5.9 and with particular reference to s.5.3.4 of these technical requirements

h) only undertake international transfers of data, taking into account the best interests of the child, in accordance with ACCS 2; s.5.10

i) in addition to the requirements of s.5.9 of these technical requirements, apply the provisions of ACCS 2: s5.11 regarding data sharing.

Note 1: *The provisions of ACCS 2; s.4.6 (Data Protection Impact Assessments), s.5.8 (Transparency), are superseded by the relevant provision of the Age Appropriate Design provisions set out in s.5 of these technical requirements.*

4.13 Scheme Clients shall establish, implement and maintain the process(es) needed to prepare for and respond to potential personal data breach situations, taking into account the best interests of the child, in accordance with ACCS 2; s.4.9.





5

Requirements for Age Appropriate Design

Requirements for Age Appropriate Design



5. Requirements for Age Appropriate Design

Best Interests of the Child

5.1.1 Scheme Clients shall ensure that they identify the needs of children and work out how they can best support those needs in the design of their online service when processing their personal data. In doing this, Scheme Clients should take into account the age of the user.

5.1.2 Scheme Clients shall ensure that they implement specific actions, in their processing and use of personal data, to secure that they:

a) keep children safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse

b) protect and support children's health and wellbeing

c) protect and support children's physical, psychological and emotional development

d) protect and support children's need to develop their own views and identity

e) protect and support children's right to freedom of association and play

f) support the needs of children with disabilities in line with the Scheme Client's obligations under the relevant equality legislation for England, Scotland, Wales and Northern Ireland

g) recognise the role of parents in protecting and promoting the best interests of the child and support parents in this task

h) recognise the evolving capacity of the child to form their own view, and give due weight to that view

Note 1: *Taking account of the best interests of the child does not mean that Scheme Clients cannot pursue their own commercial or other interests. Those commercial interests may not be incompatible with the best interests of the child, but Scheme Clients need to account for the best interests of the child as a primary consideration where any conflict arises.*

5.1.3 The Scheme Client's actions under 5.1.1 shall be documented and kept under regular review at intervals not exceeding 12 months.

Data Protection Impact Assessments

5.2.1 Scheme Clients shall ensure that they undertake a Data Protection Impact Assessment (DPIA) prior to commencing data processing.

5.2.2 The DPIA shall have a particular focus on the specific rights of and risks to children using the Scheme Client's service that arise from its data processing.

5.2.3 The DPIA shall also assess and document compliance with these technical requirements, including ensuring that the requirements are built in as additional elements into each stage of the DPIA, not bolt them on the end.

5.2.4 Scheme Clients shall embed a DPIA into the design of any new online service that is likely to be accessed by children. Scheme Clients shall also do a DPIA if they are planning to make any significant changes to the processing operations of an existing online service likely to be accessed by children.

> ***Note 1:*** *An external change to the wider context of the online service may also prompt a review of the DPIA. For example, if a new security flaw is identified, or a new public concern is raised over specific features of the online service or particular risks to children.*

5.2.5 The DPIA shall be completed before the service is launched, to ensure the outcomes can influence the design of the information society service.

> ***Note 1:*** *Scheme Clients should not treat a DPIA as a rubber stamp or tick-box exercise at the end of the design process.*

5.2.6 The DPIA shall describe the nature, scope, context and purposes of the processing. In particular, it shall include:

a) whether the service is designed for children

b) if not, whether children are nevertheless likely to access the service

c) the age range of those children

d) the plans, if any, for parental controls

e) the plans, if any, for establishing the age of their individual users

f) the intended benefits for children

g) the commercial interests (of the Scheme Client or third parties) that have been taken into account

h) any profiling or automated decision-making involved

i) any geolocation elements

j) the use of any nudge techniques

k) any processing of special category data

l) any processing of inferred data

m) any current issues of public concern over online risks to children

n) any relevant industry standards or codes of practice

o) responsibilities under the applicable equality legislation for England, Scotland, Wales and Northern Ireland

p) any relevant guidance or research on the development needs, wellbeing or capacity of children in the relevant age range

5.2.7 Scheme Clients shall seek and document the views of children and parents (or their representatives), and take them into account in their design to the extent appropriate given the size of the Scheme Client, resources and the risks identified.

> ***Note 1:*** *Larger Scheme Clients should do some form of consultation in most cases. For example, they could choose to get feedback from existing users, carry out a general public consultation, conduct market research, conduct user testing, or contact relevant children's rights groups for their views. This should include feedback on the child's ability to understand the ways their data is used and the information provided.*
>
> ***Note 2:*** *The 'representatives' of children and parents could include interest groups, civil society organisations, charities and campaign groups, in addition to representatives of individual children.*

5.2.8 A Scheme Client that establishes that it is not possible to do any form of consultation, or it is unnecessary or wholly disproportionate, shall record that decision in the DPIA, and be prepared to justify it to the Auditor.

5.2.9 Scheme Clients shall seek and review independent advice from experts in children's rights and developmental needs as part of this stage. This is especially important for services which:

a) are specifically designed for children

b) are designed for general use but known to be widely used by children (such as games or social media sites)

c) use children's data in novel or unanticipated ways

5.2.10 Scheme Clients shall ensure that they can explain why their processing is necessary and proportionate for the online service. This shall include information about how they meet the technical requirements for data protection and privacy (ACCS 2:2021), including:

a) the lawful basis for processing (see ACCS 2:2021, 5.2)

b) the conditions for processing any special category data

c) the measures to ensure accuracy, avoid bias and explain use of **AI**

d) the specific details of the technological security measures (e.g. hashing or encryption standards)

5.2.11 Scheme Clients shall identify the potential impact on children and any harm or damage the data processing may cause – whether physical, emotional, developmental or material. Scheme Clients shall also specifically identify whether the processing could cause, permit or contribute to the risk of:

a) physical harm

b) online grooming or other sexual exploitation

c) social anxiety, self-esteem issues, bullying or peer pressure

d) access to harmful or inappropriate content

e) misinformation or undue restriction on information

f) encouraging excessive risk-taking or unhealthy behaviour

g) undermining parental authority or responsibility

h) loss of autonomy or rights (including control over data)

i) compulsive use or attention deficit disorders

j) excessive screen time

k) interrupted or inadequate sleep patterns

l) economic exploitation or unfair commercial pressure

m) any other significant economic, social or developmental disadvantage

Note 1: *Scheme Clients should bear in mind children's needs and maturity can differ according to their age and development stage.*

5.2.12 To assess the level of risk, Scheme Clients shall identify both the likelihood and the severity of any impact on children. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. Scheme Clients should bear in mind that some children can be less resilient than others, so they should always take a precautionary approach to assessing the potential severity of harm. Scheme Clients may find that there is a high risk for some age ranges, even if the risk for other age ranges is lower.

5.2.13 Scheme Clients shall make changes to their service to reduce or avoid each of the risks that have been identified.

5.2.14 Scheme Clients shall identify measures that do not rely on children's ability or willingness to engage with their privacy information.

5.2.15 Scheme Clients shall seek and record the independent advice on the outcome of the DPIA before making any final decisions of either:

a) the Data Protection Officer, where the Scheme Client employs a DPO or

b) a senior person with responsibility for data protection compliance, where a DPO is not employed by the Scheme Client or

c) a third party advisor or consultant or suitably qualified legal professional

5.2.16 Scheme Clients shall record any additional measures they plan to take, and integrate them into the design of the service. In certain circumstances set out in Article 36 of UK GDPR, Scheme Clients shall be required to consult with the ICO where the DPIA for high risk data processing cannot be mitigated.

5.2.17 The DPIA shall be published on the Scheme Client's website. Sensitive information in the DPIA may be redacted in the published version.

Age Appropriate Application

5.3.1 Scheme Clients shall ensure that they conduct a risk assessment of the risks to children that arise from the processing of their personal data, which shall take into account:

a) the types of data collected

b) the volume of data

c) the intrusiveness of any profiling

d) whether decision making or other actions follow from profiling

e) whether the data is being shared with third parties

Note 1: *The risk assessment may form part of the Data Protection Impact Assessment.*

5.3.2 Scheme Clients shall take action to understand how well they know their users including assessing and documenting their levels of certainty that an individual user is an adult or a child and their levels of confidence about the age range their individual child users fall into.

5.3.3 Scheme Clients shall ensure that the level of certainty they have about the age of their individual users is appropriate to the risks that arise from the data processing. If it is, then Scheme Clients can apply the rest of these technical requirements to child users only. If it is not, then Scheme Clients shall ensure that they implement technical and organisational measures to either:

a) reduce the data risks inherent in the online service or

b) put additional measures in place to increase the level of age confidence or

c) apply these technical requirements to all users of their service (regardless of whether they have self-declared as an adult or a child)

5.3.4 Scheme Clients shall have used an appropriate method of gaining age assurance that gives the required level of assurance based on the service being accessed:

a) **self-declaration –** This is where a user simply states their age but does not provide any evidence to confirm it. It may be suitable for low risk processing or when used in conjunction with other techniques. Even if Scheme Clients prefer to apply these technical requirements to all users, self-declaration of age can provide a useful starting point when providing privacy information and age appropriate explanations of processing

b) **artificial intelligence –** It may be possible to make an estimate of a user's age by using artificial intelligence to analyse the way in which the user interacts with their service. Such mechanisms shall comply with ACCS 1 - Technical Requirements for Age Estimation Technologies and the specific requirements for the processing of special category data set out in ACCS 2; s.5.9. Similarly, this type of profiling can check that the way a user interacts with the service is consistent with their self-declared age. This technique can typically provide a greater level of certainty about the age of users with increased use of the service. If Scheme Clients choose to use this technique then they shall:

   a. notify users that they are going to do this upfront

   b. only collect the minimum amount of personal data that they need for this purpose

   c. not use any personal data collected for this purpose for other purposes

c) **third party age verification services –** Scheme Clients may use a third party service to provide them with an assurance of the age of their users. Such mechanisms shall comply with PAS 1296:2018 Code of Practice for Online Age Check Services. Such services typically work on an 'attribute' system, where the Scheme Client requests confirmation of a particular user attribute (in this case age or age range) and the service provides a 'yes' or 'no' answer. Scheme Clients shall notify the user of the identity of the age check service used for this purpose.

d) **account holder confirmation –** Scheme Clients may be able to rely upon confirmation of user age from an existing account holder who they know to be an adult. Such mechanisms shall comply with BS 8626:2020 Code of Practice for Online User Identification Systems. For example, the provision of a logged-in or subscription based service may allow the main (confirmed adult) account holder to set up child profiles,

restrict further access with a password or PIN, or simply confirm the age range of additional account users

e) **technical measures –** Scheme Clients may implement technical measures which discourage false declarations of age, or identify and close underage accounts, which may be useful to support or strengthen self-declaration mechanisms. Examples include neutral presentation of age declaration screens (rather than nudging towards the selection of certain ages), or preventing users from immediately resubmitting a new age if they are denied access to the service when they first self-declare their age

f) **hard identifiers –** Scheme Clients can confirm age using solutions which link back to formal identity documents or 'hard identifiers' such as a passport. Such mechanisms shall comply with PAS 1296:2018 Code of Practice for Online Age Check Services

Note 1: *Scheme Clients should avoid giving users no choice but to provide hard identifiers unless the risks inherent in the processing really warrant such an approach. This is because some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age verified services at all, even if they are age appropriate. Requiring hard identifiers may also have a disproportionate impact on the privacy of adults.*

5.3.5 Scheme Clients shall consider the needs of disabled children in line with any obligations that the Scheme Client has under the relevant equality legislation for England, Wales, Scotland and Northern Ireland.

5.3.6 Scheme Clients shall consider the needs of different age ranges and developmental stages of children in the design and deployment of their services.

Transparency

5.4.1 Scheme Clients shall ensure that the privacy information set out in Articles 13 and 14 is provided in a clear and prominent place on their online service.

5.4.2 Scheme Clients shall make this information easy to find and accessible for children and parents who seek out privacy information.

Note 1: *In addition to the requirements for privacy information, Scheme Clients should also provide 'bite-sized' explanations at the point at which use of personal data is activated. This is sometimes referred to as a 'just in time notice'. Depending on the age of the child and the risks inherent in the processing, Scheme Clients should also prompt them to speak to an adult before they activate any new use of their data, and not to proceed if they are uncertain.*

5.4.3 Scheme Clients shall identify any other points in their user journey when it could be appropriate to provide bite-sized explanations to aid the child's understanding of how their personal data is being used and implement those changes.

5.4.4 The Scheme Client's terms and conditions, policies and community standards shall be clear and accessible.

> ***Note 1:*** *If Scheme Clients draft terms and conditions in order to make them legally robust, then they can also provide child-friendly explanations to sit alongside the legal drafting (see further s.5.4.7).*

5.4.5 The Scheme Client's information provided shall be accurate and shall not promise protections or standards that are not routinely upheld.

5.4.6 Scheme Clients shall present all privacy information in a way that is likely to appeal to the age of the child who is accessing the online service.

> ***Note 1:*** *This may include using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that can attract and interest children, rather than relying solely on written communications.*
>
> ***Note 2:*** *Scheme Clients may use tools such as privacy dashboards, layered information, icons and symbols to aid children's understanding and to present the information in a child-friendly way. Scheme Clients should consider the modality of the service, and take into account user interaction patterns that do not take place in screen-based environments, as appropriate.*

5.4.7 Once Scheme Clients have identified the likely age groups of the users of their online services they shall:

a) when addressing children aged 0 – 5 (pre-literacy & early literacy), ensure that they provide audio or video prompts telling them to leave high privacy default settings as they are or get help from a parent or trusted adult if they try and change any. The full privacy information as required by Articles 13 & 14 of the UK GDPR shall be in a format suitable for parents

b) when addressing children aged 6 – 9 (core primary school years), ensure that they provide cartoon, video or audio materials to sit alongside parental resources. These shall explain the basic concepts of online privacy within the service, the privacy settings offered, who can see what, their information rights, how to be in control of their own information, and respecting other people's privacy

c) when addressing children aged 6 – 9 (core primary school years), explain the basics of the service and how it works, what children can expect from the Scheme Client and what

the Scheme Client expects from them. The full privacy information as required by Articles 13 & 14 of the UK GDPR shall be in a format suitable for parents

d) when addressing children aged 6 – 9, provide resources for parents to use with their children to explain privacy concepts and risks within the service and provide resources for parents to use with their children to explain the basics of the service and how it works, what they can expect from the Scheme Client and what the Scheme Client expects from them

e) when addressing children aged 6 – 9, ensure that they provide cartoon, video or audio materials to explain to the children what can happen to their information and any associated risks, and to leave high privacy default settings as they are or get help from a parent or trusted adult if they try and change any

f) when addressing children aged 10 – 17 (Transition years through to approaching adulthood), provide full privacy information as required by Articles 13 & 14 of the UK GDPR in a format suitable for them. In addition, Scheme Clients shall provide full privacy information as required by Articles 13 & 14 of the UK GDPR in a format suitable for parents

g) when addressing children aged 10 – 17 (Transition years through to approaching adulthood), allow them to choose between written and video/audio options and give these children the choice to upscale or downscale the information they see (to materials developed for an older or younger age group) depending on their individual needs

h) when addressing children aged 10 – 17 (Transition years through to approaching adulthood), ensure that they provide written and video/audio materials to explain what can happen to their information and any associated risks, and to leave high privacy default settings as they are or get help from a parent or trusted adult if they try and change any

5.4.8 Dashboards shall be displayed in a way that clearly identifies and differentiates between processing that is essential to the provision of the service and non-essential or optional processing that the child can choose whether to activate.

5.4.9 Scheme Clients shall ensure that they identify how to tailor the content and presentation of the information provided depending on the age of the user. For younger children, with more limited levels of understanding, Scheme Clients may need to provide less detailed information for the child themselves and rely more on parental involvement and understanding.

5.4.10 Scheme Clients shall not use simplification with the aim of hiding what they are doing with the child's personal data.

5.4.11 Scheme Clients shall provide detailed information for parents, to sit alongside information directed at children.

5.4.12 Scheme Clients shall make all versions of resources (including versions for parents) easily accessible and incorporate mechanisms to allow children or parents to choose which version they see, or to down-scale or up-scale the information depending on their individual level of understanding.

> ***Note 1:*** *Depending on the size of the Scheme Client, the number of users and the assessment of risk, Scheme Clients may decide to carry out user testing to make sure that the information provided is sufficiently clear and accessible for the age range in question. They should document the results of any user testing in the DPIA to support their final conclusions and justify the presentation and content of their final resources. If Scheme Clients decide that user testing is not warranted, then they should document the reasons why in their DPIA.*

5.4.13 Scheme Clients shall ensure that they identify and address any additional responsibilities they have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland.

Detrimental Use of Data

5.5.1 Scheme Clients shall ensure that they are aware of and document the relevant standards and codes of practice within their industry or sector, and any provisions within them that relate to children.

> ***Note 1:*** *Relevant standards include those issued by the Advertising Standards Authority, OFCOM, Portman Group Codes, Betting and Gaming Council Codes, Competition and Markets Authority or any other appropriate industry standards, codes or best practice.*

5.5.2 Scheme Clients shall not process children's personal data in ways that are obviously detrimental or run counter to such advice.

5.5.3 Scheme Clients should take account of any age specific advice to tailor their online service to the age of the child.

5.5.4 Scheme Clients shall take particular care when profiling children, including making inferences based on their personal data, or processing geo-location data.

5.5.5 Scheme Clients shall not process children's personal data in ways that have been formally identified as requiring further research or evidence to establish whether or not they are detrimental to the health and wellbeing of children.

5.5.6 Scheme Clients shall identify and address, through appropriate risk assessment and mitigation, any aspects of their online services that risks:

a) physical, mental or moral harm to children

b) exploiting children's credulity and applying unfair pressure, including aggressive commercial practices

c) direct exhortation of children and undermining parental authority

d) prohibited marketing of certain products, such as high fat, salt and sugar food and drinks and alcohol, to children, and general guidance on transparency of paid-for content and product placement

e) exposure to strategies used to extend user engagement, sometimes referred to as 'sticky' features, which can include mechanisms such as reward loops, continuous scrolling, notifications and auto-play features which encourage users to continue playing a game, watching video content or otherwise staying online

f) exposing the coverage of sexual and other offences in the UK involving under-18s

g) exposing drugs, smoking, solvents and alcohol

h) exposing violence and dangerous behaviour

i) exposing offensive language

j) exposing sexual material

k) exposing nudity

l) exposing exorcism, the occult and the paranormal

m) the involvement of people under 18 in broadcast programmes

5.5.7 Scheme Clients shall not:

a) use features which use personal data to exploit human susceptibility to reward, anticipatory and pleasure seeking behaviours, or peer pressure

b) use personal data in a way that incentivises children to stay engaged, such as offering children personalised in-game advantages (based upon the service's use of the individual user's personal data) in return for extended play

c) present options to continue playing or otherwise engaging with the service neutrally by suggesting that children can lose out if they stop playing

d) use personal data to automatically extend use instead of requiring children to make an active choice about whether they want to spend their time in this way (data-driven autoplay features)

5.5.8 Scheme Clients shall introduce mechanisms such as pause buttons which allow children

to take a break at any time without losing their progress in a game, or provide age appropriate content to support conscious choices about taking breaks.

Policies and Community Standards

5.6.1 Scheme Clients shall comply with their side of any requirements in their own policies and community standards.

> ***Note 1:*** *Particular attention is drawn to ACCS 2; s.5.2.3 regarding any deceptive or misleading statements made during the collection and processing of personal data. Processing otherwise than in accordance with their own policies and community standards can result in unfair processing.*

5.6.2 As required by s. 4.12 (b) & (c) of these technical requirements, Scheme Clients shall comply with the purpose limitation requirements of ACCS 2; ss. 5.3 & 5.4, taking into account the best interests of the child.

5.6.3 Scheme Clients shall implement and enforce any of their rules which govern the behaviour of users of their service. This includes any promises to actively monitor user behaviour, offer real time, automated, or human moderation of 'chat' functions.

5.6.4 Scheme Clients that rely on 'back end' processes such as user reporting to identify behaviour which breaches their policies, shall have made that clear in their policies or community standards. This approach shall be reasonable given the risks to children of different ages inherent in the online service. If the risks are high then 'light touch' or 'back end only' processes to uphold their standards shall not be sufficient.

5.6.5 Scheme Clients shall implement and enforce any of their rules for users about the content or other aspects of the online service. So if Scheme Clients say that the content of the online service is suitable for children within a certain age range then they shall have systems to ensure that it is. If they say that they do not tolerate bullying, then they shall have adequate mechanisms to swiftly and effectively deal with bullying incidents.

5.6.6 Scheme Clients that have different policies depending on the age of the users shall take account of the age of the child when upholding their policies.

Default Settings

5.7.1 Scheme Clients shall set the privacy settings by default to 'high privacy' and ensure that children's personal data is only visible or accessible to other users of the service if the child amends their settings to allow this. A Scheme Client may demonstrate that there is a compelling reason for a different default setting taking into account the best interests of the child.

5.7.2 Scheme Clients shall ensure that unless the setting is changed, their own use of the children's personal data is limited to use that is essential to the provision of the service.

Any optional uses of personal data, including any uses designed to personalise the service, shall be individually selected and activated by the child.

5.7.3 Any settings which allow third parties to use personal data shall be activated by the child.

5.7.4 Scheme Clients shall implement further measures when a child attempts to change a default privacy setting.

> ***Note 1:*** *This could include further age assurance measures. Scheme Clients should use their DPIA to help them assess risks and identify suitable mitigation.*

5.7.5 Scheme Clients shall allow users the option to change settings permanently or just for the current user session.

5.7.6 Scheme Clients shall be able to demonstrate that they have made it easy for a child to maintain or revert to high privacy settings if they wish to do so.

5.7.7 Scheme Clients that update or upgrade software shall retain user choices. If it is not possible to do this (e.g. if a new aspect or feature to the product or service is introduced, or an existing feature is significantly changed so the previous privacy settings are no longer relevant), the new setting shall be to high privacy by default.

5.7.8 Where Scheme Clients offer multi-user profiles, they shall allow for different user choices on multi-user devices. If Scheme Clients provide an online service that allows multiple users to access the service from one device, then they shall allow users to set up their own profiles with their own individual privacy settings. This means that children do not have to share an adult's privacy settings when they share the same device.

> ***Note 1:*** *Profiles could be accessed via screen-based options or using voice recognition technology for voice activated online services.*

5.7.9 Scheme Clients shall provide clear information for the person who sets up or registers the device, alerting them to the potential for the personal data of multiple users to be collected.

5.7.10 Where a Scheme Client has settings off by default and the user has to activate the processing by changing the default setting, then Scheme Clients shall provide mechanisms for obtaining consent to the processing under the UK GDPR, such as using privacy settings as part of their mechanism. However, they shall also meet the requirements of Article 7 of the UK GDPR (conditions for consent) and the age verification and parental responsibility verification requirements of Article 8 (under UK GDPR, these only allow children of 13 or over to provide their own consent), so they may not be enough on their own.

> ***Note 1:*** *Scheme Clients may also use privacy settings to give children choice over how their personal data is used if the Scheme Client relies on other lawful bases for processing (such as legitimate interests) which do not have any formal consent requirements.*

Data Minimisation

5.8.1 Scheme Clients shall only collect and process personal data that is adequate, relevant and necessary for the purposes for which they are processed.

5.8.2 Scheme Clients shall give children choice over which elements of the service they wish to use and therefore how much personal data they need to provide.

5.8.3 Scheme Clients shall not 'bundle in' the collection of children's personal data in order to provide enhancements with the collection of personal data needed to provide the core service. Neither shall Scheme Clients bundle together several additional elements or enhancements of the service. Scheme Clients shall give children a choice as to whether they wish their personal data to be used for each additional purpose or service enhancement.

5.8.4 Scheme Clients shall only collect personal data when the child is actively and knowingly using that element of the service.

Data Sharing

5.9.1 Scheme Clients shall ensure that the best interests of the child are a primary consideration whenever contemplating sharing children's personal data.

> ***Note 1:*** *There are further requirements relating to data sharing set out in s.5.11 of ACCS 2 and Scheme Clients should also apply the provisions of the Data Sharing Code.*

5.9.2 Scheme Clients shall not share personal data if it can reasonably be foreseen that doing so can result in third parties using children's personal data in ways that have been shown to be detrimental to their wellbeing.

5.9.3 Scheme Clients shall obtain assurances from whoever they share the personal data with about the restriction on use of the data and protecting the child's wellbeing, and should only share the child's data if there is a compelling reason to do so.

> ***Note 1:*** *One clear example of a compelling reason is data sharing for safeguarding purposes, preventing child sexual exploitation and abuse online, or for the purposes of preventing or detecting crimes against children such as online grooming.*
>
> ***Note 2:*** *An example that is unlikely to amount to a compelling reason for data sharing is selling on children's personal data for commercial re-use.*

5.9.4 Scheme Clients shall undertake due diligence checks on third parties as to the adequacy of their data protection practices and any further distribution of the data.

5.9.5 Any default settings related to data sharing shall specify the purpose of the sharing and who the data can be shared with.

5.9.6 Any settings which allow general or unlimited sharing shall not be permitted.

5.9.7 Scheme Clients shall identify the specific issues and risks of data sharing at each individual stage of their DPIA.

Geolocation

5.10.1 Scheme Clients shall ensure that geolocation options are off by default.

5.10.2 Children shall only be required to change the default geolocation setting if they want to activate the geolocation functions. The exception to this is if the Scheme Client can demonstrate a compelling reason for a geolocation option to be switched on by default, taking into account the best interests of the child. For example they may be able to argue that metrics needed to measure demand for regional services may be sufficiently un-intrusive to be warranted (taking into account the best interests of the child).

5.10.3 Scheme Clients shall identify at what level of granularity the location needs to be tracked to provide each element of the service.

5.10.4 Scheme Clients shall not collect more granular detail than is actually needed, and shall offer different settings for different levels of service if appropriate.

5.10.5 Scheme Clients shall provide information at the point of sign-up on location tracking, and each time the service is accessed, that alerts the child to the use of geolocation data and prompts them to discuss this with a trusted adult if they do not understand what it means.

5.10.6 Scheme Clients shall provide a clear indication of when the child's location is and is not being tracked (e.g. by use of a clear symbol visible to the user), and ensure that location tracking cannot be left on inadvertently or by mistake.

5.10.7 Scheme Clients shall ensure that they revert settings which make the child's location visible to others to 'off' after each use. The exception to this is if the Scheme Client can demonstrate that they have a compelling reason to do otherwise, taking into account the best interests of the child.

Parental Controls

5.11.1 Scheme Clients shall ensure that they make it clear to the child if parental controls are in place and if they are being tracked or monitored.

> ***Note 1:*** *Parental monitoring impacts upon the privacy of children. This may or may not be detrimental to the best interests of the child. The expectation of privacy for children is likely to increase as they get older.*

5.11.2 If the online service allows parental monitoring or tracking of a child, Scheme Clients shall

provide age appropriate resources to explain the service to the child so that they are aware that their activity is being monitored by their parents or their location tracked.

5.11.3 Scheme Clients shall provide a clear and obvious sign for the child (such as an illuminated icon) which lets them know when monitoring or tracking is active.

5.11.4 Scheme Clients shall provide parents with information about the child's right to privacy under the UNCRC and resources to support age appropriate discussion between parent and child.

5.11.5 Scheme Clients shall identify and address any additional responsibilities they may have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland.

5.11.6 Scheme Clients shall ensure that they provide audio or video prompts (or for older children written materials) explaining to children that their parent is being told what they do online to help keep them safe.

5.11.7 Scheme Clients shall provide materials for parents explaining the child's right to privacy under the UNCRC and how their expectations about this are likely to increase as they get older. This can include resources to help parents explain the service to their child and discuss privacy with them and resources suitable for older children to use independently which explain the service and discuss privacy rights.

Profiling

5.12.1 Scheme Clients shall ensure that they differentiate between different types of profiling for different purposes.

> ***Note 1:*** Catch-all purposes, such as 'providing a personalised service' are not specific enough.

5.12.2 Where it is appropriate to offer privacy settings, then the Scheme Client shall offer separate settings for each different type of profiling.

5.12.3 Scheme Clients shall not bundle different types of profiling together under one privacy setting, or bundle in profiling with processing for other purposes.

5.12.4 Scheme Clients shall ensure that features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise, taking account of the best interests of the child).

> ***Note 1:*** *Scheme Clients may have a compelling argument for their need to switch profiling options for other purposes on by default. For example, it may be appropriate for profiling for the purposes of ensuring that a service is accessible to a disabled child (e.g. identifying that a child has an ongoing need for a subtitled, signed or other supported service) to be switched on by default.*

Note 2: *Scheme Clients may be able to demonstrate that profiling for the purposes of informing news content feeds should be allowed by default, in order to recognise the rights of children to access information. Although Scheme Clients may still need consent to set the cookies that support the profiling.*

Note 3: *This is more likely to be the case if the Scheme Client can demonstrate that they conform with existing regulatory codes of practice which govern media content and practices (such as The Editors' Code of Practice) and have editorial control over the content that children can be shown as a result of the profiling. It is unlikely to apply if they do not have such editorial control or adhere to other regulatory controls.*

5.12.5 Any Scheme Client that undertakes profiling for the purposes of behavioural advertising, which is facilitated by cookies, shall ensure that valid consent is obtained by an 'opt in' option. Scheme Clients shall not allow such profiling 'by default'.

Note 1: *Scheme Clients also need to comply with the Article 8 UK GDPR requirements for parental consent if the child is under the age of 13 (under UK GDPR).*

5.12.6 Scheme Clients shall provide appropriate interventions at the point at which any profiling is activated, including providing age appropriate information about what can happen to the child's personal data and any risks inherent in that processing.

5.12.7 Scheme Clients shall provide age appropriate prompts to seek assistance from an adult and not to activate the profiling if they are uncertain or do not understand.

5.12.8 Where profiling is switched on, Scheme Clients shall ensure that they put appropriate measures in place to safeguard the child (in particular from inappropriate content) and ensure the profiling does not result in any harm to the child.

Note 1: *In practice this means that if the Scheme Client profiles children (using their personal data) in order to suggest content to them, then they need suitable measures in place to make sure that children are not served content which is detrimental to their physical or mental health or wellbeing, taking into account their age. As covered in the section of this code on DPIAs, testing the algorithms should assist in assessing the effectiveness of the measures put in place.*

Note 2: *Such measures could include contextual tagging, robust reporting procedures, and elements of human moderation. It could also include editorial controls over the content displayed, including adherence to codes of conduct or other regulatory provisions (such as compliance with The Editors' Code of Practice, or the Ofcom Broadcasting Code). Children have an important right to access information from the media, and the societal and developmental benefits of children being able to engage in current affairs and the world around them. Adherence to editorial or broadcasting codes*

of conduct can negate the need for providers of online news to take any additional steps in relation to news content for children.

5.12.9 Scheme Clients that are using children's personal data to automatically recommend content to them based on their past usage/browsing history shall be responsible for the recommendations made. This applies even if the content itself is user generated.

> ***Note 1:*** *In data protection terms, Scheme Clients have a greater responsibility in this situation than if the child were to proactively search out such content themselves. This is because it is the Scheme Client's processing of the personal data that serves the content to the child. Data protection law does not make the Scheme Client responsible for third party content but it does make them responsible for the content they serve to children who use their service, based on the use of their personal data.*

5.12.10 Scheme Clients shall ensure that if the content they promote or the behaviours their system features encourage are obviously detrimental, or are recognised as harmful to the child in one context (e.g. marketing rules, film classification, advice from official Government sources such as Chief Medical Officers' advice, PEGI ratings), then they shall assume that the same type of content or behaviour is harmful in other contexts as well. Where evidence is inconclusive, Scheme Clients should apply the same precautionary principle.

5.12.11 Scheme Clients shall take into account content or behaviours that may be detrimental to children's health and wellbeing (taking into account their age) including:

a) advertising or marketing content that is contrary to CAP guidelines on marketing to children

b) film or on-demand television content that is classified as unsuitable for the age group concerned

c) music content that is labelled as parental advisory or explicit

d) pornography or other adult or violent content

e) user generated content (content that is posted by other internet users) that is obviously detrimental to children's wellbeing or is formally recognised as such (e.g. pro-suicide, pro-self harm, pro-anorexia content, content depicting or advocating risky or dangerous behaviour by children)

f) strategies used to extend user engagement, such as timed notifications that respond to inactivity

5.12.12 Scheme Clients that are not able to put suitable measures in place to safeguard children from harmful content or behaviour shall not profile children for the purposes of recommending online content. In these circumstances Scheme Clients shall ensure that children cannot change any privacy settings which allow this type of profiling.

5.12.13 Scheme Clients shall take account of other rules on restricting access to content in order to ensure that they do not use children's personal data in ways that have been shown to be detrimental to their wellbeing.

> ***Note 1:*** *The CAP code requires that when advertising is targeted through the use of personal data, advertisers shall show that they have taken reasonable steps to reduce the likelihood of those who are, or are likely to be, in a protected age category being exposed to age-restricted marketing content.*
>
> ***Note 2:*** *The Ofcom On Demand Programme Service Rules require providers of 'on demand' content to only make certain content ('specially restricted material') available, if it can do so in a way that ensures that those under the age of 18 should not normally be able to see or hear it.*
>
> ***Note 3:*** *The Communications Act 2003 (as amended by various Audio Visual Media Services Regulations) requires 'video sharing platform services' to use proportionate measures in relation to how they organise the content they share, to protect minors from content which might impair their physical, mental or moral development.*

5.12.14 Scheme Clients shall only allow children's personal data to be used to determine content feeds if they can put suitable measures in place to guard against them being served content that is detrimental to their health and wellbeing.

5.12.15 Scheme Clients shall not use personal data collected or generated for the purposes of protecting minors from content which might impair their physical, mental or moral development for commercial purposes such as direct marketing, profiling and behaviourally targeted advertising.

5.12.16 Scheme Clients shall provide users with clear and comprehensive information about the use of cookies and obtain prior consent for any that are 'non-essential'.

> ***Note 1:*** *If the child decides to access non-core services, then consent for the use of the cookie is not needed – as the child is specifically requesting to access part of the service and the cookie is strictly necessary for this purpose. Scheme Clients do however need a lawful basis for the underlying processing.*

5.12.17 Scheme Clients shall identify and record a lawful basis for processing for any cookie that is essential to the provision of the core service. Consent is not an appropriate lawful basis where the processing is essential to the core service provided.

> ***Note 1:*** *If the cookie is essential to the provision of the Scheme Client's core service then it is likely that the underlying profiling that the cookie enables is too. In this circumstance providing a privacy setting which allows the child to control whether their personal data is used for this purpose will not be appropriate.* The Scheme Client should

identify a lawful basis (other than consent) for the underlying processing (profiling) and will not need consent for the cookie.

5.12.18 Scheme Clients may use cookies for profiling that intends to meet the implied age verification requirements of Article 8 of the UK GDPR, or to age assure in order to properly apply the standards of this Code. If they do, the purpose for the use of the cookies is regarded as essential for the service, as they need to do so to provide an age appropriate service and comply with the UK GDPR. Provided that the cookie in question is solely used for this purpose, and not for any other purpose, then the child does not need to consent to the cookie.

Nudge Techniques

5.13.1 Scheme Clients shall not use nudge techniques to lead or encourage children to activate options that mean they give the Scheme Client more of their personal data, or turn off privacy protections.

5.13.2 Scheme Clients shall not exploit unconscious psychological processes to this end (such as associations between certain colours or imagery and positive outcomes, or human affirmation needs).

5.13.3 Scheme Clients shall not use nudge techniques that might lead children to lie about their age. For example pre-selecting an older age range for them, or not allowing them the option of selecting their true age range.

5.13.4 Taking into account the best interests of the child as a primary consideration, Scheme Clients shall ensure that their design supports the developmental needs of the age of their child users.

> ***Note 1:*** *Younger children, with limited levels of understanding and decision making skills, need more instruction based interventions, less explanation, unambiguous rules to follow and a greater level of parental support. Nudges towards high privacy options, wellbeing enhancing behaviours and parental controls and involvement should support these needs.*

> ***Note 2:*** *As children get older the focus should gradually move to supporting them in developing conscious decision making skills, providing clear explanations of functionality, risks and consequences. They can benefit from more neutral interventions that require them to think things through. Parental support may still be required but should be presented as an option alongside signposting to other resources.*

5.13.5 Where appropriate, Scheme Clients should nudge children in ways that support their health and wellbeing. For example, nudging them towards supportive resources or providing tools such as pause and save buttons.

Note 1: *If Scheme Clients use personal data to support these features then they still need to make sure their processing is compliant (including having a lawful basis for processing and have provided clear privacy information), but subject to this it is likely that such processing can be fair.*

5.13.6 Scheme Clients shall identify, document and address any additional responsibilities they may have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland.

5.13.7 Scheme Clients shall provide design architecture which is high-privacy by default for children.

Note 1: *If a change of default is attempted by younger children, Scheme Clients should nudge towards maintaining high privacy or towards parental or trusted adult involvement.*

5.13.8 For younger children, Scheme Clients shall avoid explanations and instead present as rules to protect and help. They shall identify further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks inherent in the processing.

Note 1: *The Code provides a specific table that suggests specific measures for younger and older children, that Scheme Clients should apply in complying with this provision.*

5.13.9 Scheme Clients shall nudge towards wellbeing enhancing behaviours (such as taking breaks) and provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).

5.13.10 For older children, Scheme Clients shall provide simple explanations of functionality and inherent risk, but continue to present as rules to protect and help. They shall identify further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks inherent in the processing.

5.13.11 For older children, Scheme Clients shall present options in ways that encourage conscious decision making.

Note 1: *The Code provides a specific table that suggests specific measures for younger and older children, that Scheme Clients should apply in complying with this provision.*

Connected Toys and Devices

5.14.1 Scheme Clients that provide a connected toy or device shall identify who is processing the personal data that it transmits via the network connection and what their data protection responsibilities are.

5.14.2 Scheme Clients that provide both the physical product and the online functionality that supports it, are solely responsible for ensuring compliant processing.

> ***Note 1:*** *If the Scheme Client outsources or 'buys in' the online functionality or 'connected' element of the device, then whoever provides this aspect of the overall product shall also have responsibilities. The extent of these can vary depending on whether they are a 'processor' acting only on behalf of the Scheme Client, or a 'controller' in their own right.*
>
> ***Note 2:*** *However, Scheme Clients cannot absolve themselves of their data protection obligations by outsourcing the 'connected' element of the toy or device to someone else. If they provide a connected toy or device then they need to comply with the UK GDPR and follow these technical requirements, and make sure that any third parties they use to deliver their overall product do so too.*

5.14.3 Scheme Clients shall ensure that the product incorporates adequate security measures to mitigate risks such as unauthorised access to data, or 'hacking' of the device in order to communicate with the child (e.g. taking over microphone capabilities) or track their location.

5.14.4 Scheme Clients that provide a connected device shall anticipate and provide for it to be used by multiple users of different ages and shall:

a) ensure that the service that they provide by default (the service that would be provided, for example, to occasional visitors to a household) is suitable for use by all children

b) provide user profile options for people who use the device regularly (e.g. household members and frequent visitors to a household) to support use by adults, or to tailor the service to the age of a particular child

> ***Note 1:*** *This is particularly the case for devices such as home hub interactive speaker devices which are likely to be used by multiple household members, including children, and may also be used by visitors to the home. Similarly, interactive toys are often shared or may be used by several children at once when they play together.*

5.14.5 Scheme Clients shall provide clear information indicating that the product processes personal data at the point of sale and prior to device set-up. Both the packaging of the physical product, and the product leaflet or instruction booklet (paper or digital) should carry a clear indication (such as an icon) that the product is 'connected' and processes users' personal data.

5.14.6 Scheme Clients shall allow potential purchasers to view the Scheme Client's privacy information, terms and conditions of use and other relevant information online without having to purchase and set up the device first, so that they can make an informed decision about whether or not to buy the device in the first place.

Note 1: *Scheme Clients should also have a particular focus on the tools they provide to facilitate the set-up of the connected toy or device. This is a key opportunity for them to provide information about how the service works, how personal data is used and to explain the implications of this, especially if set-up is activated using a screen-based interface. If the child's ongoing use of the device is not screen-based this is particularly important as this may limit the ways in which Scheme Clients can convey information to the child on an ongoing basis.*

5.14.7 Scheme Clients shall identify and address how the connected device operates and how best to communicate 'just in time' information to the child or their parent. This may include auto-play audio messages, only allowing default settings to be changed via use of a support app, or facilitating interactive auto-bot 'conversations' with the user.

5.14.8 Scheme Clients shall provide features that make it clear to the child or their parent when the device is collecting personal data. For example a light that switches on when the device is audio recording, filming or collecting personal data in another way.

5.14.9 If the device uses a stand-by or 'listening' mode (e.g. it listens out for the name the Scheme Client or the child has given to the device, or for another key word or phrase to be used, and activates data collection when that word or phrase is used), Scheme Clients shall provide a clear indication that listening mode is active.

5.14.10 Scheme Clients shall not collect personal data when the device is in listening mode.

5.14.11 Scheme Clients shall provide features which allow collection or listening modes to be easily switched off on the device itself (a 'connection off' button), or via online functionality options, so that the toy or device can be used as a non-connected device so far as this is practicable.

Online Tools

5.15.1 Scheme Clients shall provide online tools that enable children to exercise their rights and report concerns to the Scheme Client.

Note 1: *See ACCS 2, s.5.7 for additional requirements on data subject's rights, however, these technical requirements are intended to ensure that Scheme Clients develop age appropriate tools for children to exercise their rights and report concerns.*

5.15.2 Scheme Clients shall make their online 'rights' tools prominent and easy for children to find.

5.15.3 Scheme Clients shall highlight the reporting tool (such as tools to report concerns, flag inappropriate conduct or behaviour) in their set up process and provide a clear and easily identifiable icon or other access mechanism in a prominent place on the screen display.

Note 1: *If the online service includes a physical product, for example a connected toy or speaker, the Scheme Client can include the icon on their packaging, highlighting online reporting tools as a product feature, and find ways to highlight reporting tools in a prominent way even if the product is not screen-based.*

5.15.4 Scheme Clients shall make their online tools age appropriate and easy to use.

5.15.5 Scheme Clients shall tailor their online tools to the age of the child in question.

5.15.6 Scheme Clients shall identify and address any additional responsibilities they may have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland.

5.15.7 Scheme Clients shall provide icon(s), audio prompts or similar that even the youngest of children can recognise as meaning 'I'm not happy' or 'I need help'. If these buttons are pressed, or other prompts responded to, Scheme Clients shall provide video or audio material prompting the child to get help from a parent or trusted adult.

5.15.8 Scheme Clients shall provide online tools for safeguarding children suitable for use by parents, or for older children provide online tools that children could use either by themselves or with the help of an adult.

5.15.9 Scheme Clients shall provide icon(s), audio prompts or similar that older children can recognise as meaning 'I want to raise a concern', 'I want to access my information' or 'I need help'. If these buttons are pressed, or other prompts responded to, Scheme Clients shall direct the child to the online tools and prompt them to get help from a parent or other trusted resource if they need it.

5.15.10 Scheme Clients shall provide age appropriate tools to support the rights children have under the UK GDPR. For example:

a) a 'download all my data' tool to support the right of access, and right to data portability

b) a 'delete all my data' or 'select data for deletion' tool to support the right to erasure

c) a 'stop using my data' tool to support the rights to restrict or object to processing

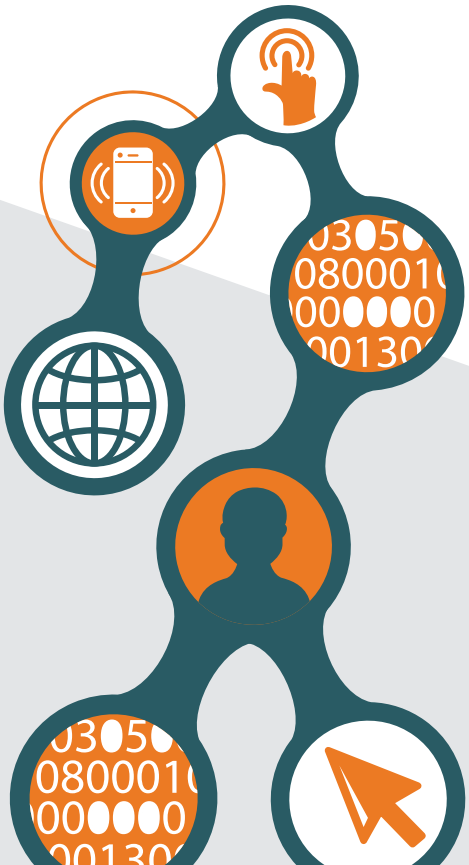
d) a 'correction' tool to support the right to rectification

5.15.11 Scheme Clients shall establish online tools that include ways for the child or their parent to track the progress of their complaint or request, and communicate with the Scheme Client about what is happening.

5.15.12 Scheme Clients shall provide information about their timescales for responding to requests from children to exercise their rights, and shall deal with all requests within the timescales set out at Article 12(3) of the UK GDPR.

5.15.13 Scheme Clients shall have mechanisms for children to indicate that they think their complaint or request is urgent and why, and the Scheme Clients shall actively identify any information they provide in this respect and prioritise accordingly.

5.15.14 Scheme Clients shall ensure that they have procedures in place to take swift action where information is provided indicating there is an ongoing safeguarding issue.







© Age Appropriate Design Certification Scheme

Visit us on social media...

@AgeCheckCert





Internationally recognised standards

Our scheme provides evidence that identity and age check practices meet international standards.



Highly qualified certification officers

Our locally trained certification officers are highly qualified professionals in each jurisdiction.



Evidence you can use to demonstrate compliance

Our certificates of conformity are internationally recognised by law enforcement.



Guaranteed independence & impartiality

Our independent board, impartiality committee and ISO processes guarantee impartial certification.

Age Check Certification Scheme

www.accscheme.com

An independent not-for-profit company registered in England and Wales (11493870) at Unit 321B Broadstone Mill, Broadstone Road, Stockport, SK5 7DL

ISBN 978-1-7398513-3-0

0 638266 208955