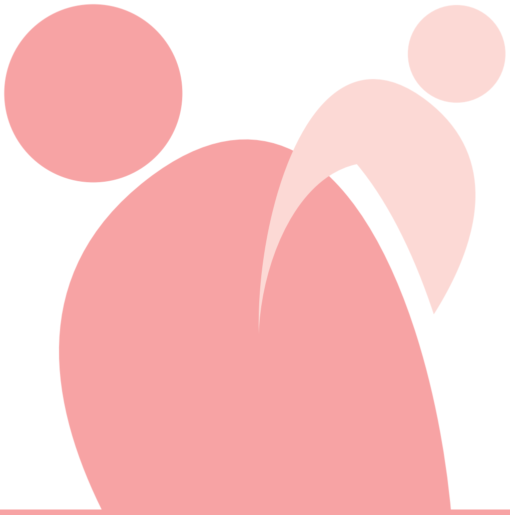
VoCO (Verification of Children Online)
Phase 2 Report



"If platforms could verify which of their users were children, then as a society we would be better empowered to protect children from harm as they grow up online..."

November 2020

GCHQ

Counter Child Sexual Abuse

ACE

ACCELERATED CAPABILITY ENVIRONMENT

Powered by vivace

Department for Digital, Culture, Media & Sport

Home Office

The VoCO project has been undertaken by GCHQ, led by DCMS and supported by the Home Office.

GCHQ has undertaken VoCO in partnership with ACE, to take forward their goal of protecting children from sexual abuse online.

- GCHQ has avowed their work to reduce the harm from child sexual abuse and to make children safer online.
- DCMS is leading VoCO as part of their commitment to protect children, which is at the heart of the Online Harms agenda.
- DCMS seeks to boost innovation and promote technology solutions in the 'age assurance' space. Insights and research resulting from VoCO will inform ongoing work in this area.
- The Home Office is supporting the VoCO project because they recognise the importance of platforms knowing the age of their users as a key component to tackle online grooming.
- The Home Office's Accelerated Capability Environment (ACE) solves fast-changing digital and technological challenges facing law enforcement and national security agencies.

VoCO Phase 2 is a multi-stakeholder research project. It is important to note that this is a report of the findings made through this project and should not be read as a blueprint for government's next steps on age assurance.

Executive Summary

VoCO (Verification of Children Online) is a child online safety research project that responds to the challenge of knowing which online users are children. It is motivated by the hypothesis that children's online safety and wellbeing will be improved if we have an internet that actively recognises children and adapts the spaces they use to make them safer by design.

"If platforms could verify which of their users were children and establish parental consent, then as a society we would be better empowered to protect children from harm as they grow up online" - the original[1] VoCO hypothesis.

Technology has an important role to play in protecting children online. In the context of the VoCO project, technical measures to establish the age of users plays a key part in bringing about VoCO's objectives. The project developed the concept and definition of age assurance as a term to describe the broad range of technical measures that can be used by a service to establish the age of their users. Acknowledging this breadth has been important for progressing the discussion about recognising children online. For this reason, we use the definition of age assurance in this report to discuss the full spectrum of methods that can be used to establish the age of users and actively recognise child users in a way that enhances their online experience, rather than blocking them.

The Problem

The internet wasn't designed for children, but a third of all internet users globally are under 18.[2] It is these children who are driving the change in how we socialise, play and express ourselves online. Yet it is children who are disproportionately affected by the risks of going online.

> **Social media is now a ubiquitous part of childhood, but alongside wonderful opportunities, it opens up an array of potential harms…Being online has become the norm for the majority of children, so to them, it is their 'real life'**
>
> **– NSPCC, Wild West Web Campaign**

The UK's Online Harms White Paper highlights that 99% of 12-15 year olds in the UK are going online, spending an average of twenty and a half hours a week on the internet.[3] It is important to remember that the internet offers many benefits for children. It provides them with access to learning opportunities, entertainment and the ability to stay in touch with family and friends. All of this is important for their wellbeing, opportunities and development. However, the internet does present risks to children and some do encounter online content and behaviour that is harmful to them, and in some cases illegal.

Research undertaken by Ofcom last year found that 79% of 12-15 year olds surveyed reported that they have had at least one potentially harmful experience online in the past 12 months and seven in ten 12-15 year olds (71%) mentioned potential harm relating to interaction with other people and/or content.[4] Sadly, children can experience many forms of online harm, one of the most damaging being online Child Sexual Exploitation and Abuse (CSEA). This is a persistent challenge. In 2019, 74,330 UK-related referrals were made to the National Center for Missing and Exploited Children (NCMEC).[5] In 2019, over a period of just three months, Facebook reported removing 11.6 million pieces of content globally for breaching policies on child nudity and sexual exploitation.[6]

The scale of online CSEA necessitates collaboration, cooperation and innovation across government, industry, academia and civil society to tackle it.

The unique situation of the covid-19 pandemic has put in the spotlight the risk posed to children online. With many more children at home and online for education and socialising there was universal concern that this may put some at an increased risk of experiencing harm. Europol reported in June that there had been a significant increase in communications on dark web offender forums since global lockdowns, with the average

[1] As the VoCO project matured, the emphasis on parental consent became less of a focus, as the concept is built around empowering children and ensuring that they are protected by default, reducing the burden on digital parents (especially in situations where digital parents are not engaged).

[2] Unicef, 'One in Three: Internet Governance and Children's Rights', 2016

[3] HM Government, 'Online Harms White Paper,' 2019

[4] Ofcom, ICO, 'Internet users' concerns about and experience of potential online harms', 2019

[5] NCMEC, '2019 Reports by Country', 2020

[6] BBC, 'Facebook removes 11.6 million child abuse posts', 2019

number in some forums tripling.[7] These message forums are focused on up-skilling offenders in new or improved means of targeting children. SafeToNet estimates that there has been an average 183% rise in UK children using sexual language since the beginning of lockdown. Girls aged 11, and boys aged 13 are the most likely to engage in this behaviour, on an increasing number of platforms.[8] At time of publishing this report the relationship between covid-19 and child online safety is a live issue with work ongoing by government and law enforcement to understand and respond to the threat.

Our Findings

Through the VoCO project we have attempted to capture the experiences and needs of children and parents, and to identify what landscape and incentives are needed for platforms to start age assuring their users.

Child users, parents and platforms.

An important consideration of VoCO has been the relationship between child users, their parents, and the platforms that they use. The project sought to understand the current dynamic between these groups, understanding why and how it was failing, and to establish what relationships are needed between these groups. A detailed description of the situation for children and their digital parents can be found in Appendix 3.

Our research found that children commonly lie about their age to access platforms that appeal to them.[9] This situation has been encouraged by the current regulatory landscape, which the largest and predominantly US based platforms are subject to. The Children's Online Privacy Protection Act (COPPA, US 2000) has been a significant piece of child safety legislation; its goal being that for children 13 or under their parents are placed in control over what data is collected about them. However, its implementation has had the unintended consequence of disincentivising platforms from actively recognising which of their users are children and designing age appropriate environments for them. This has impacted not just in the US but also globally. Many of the largest general use platforms are based in the US, and the operational decisions that they take in order to comply with COPPA have an impact on children around the world. Platforms become subject to COPPA's rules if they have actual knowledge that they have users that are under 13. To avoid exposure to COPPA many platforms have adopted age-screening mechanisms. However, these methods overwhelmingly rely exclusively on the user self-asserting their age, placing the responsibility for attesting age onto the child. Children are incentivised to lie in order to bypass restrictions or parental consent requirements. This has created an incongruence between the intended audience and actual audience on a platform. Consequently it is normal for children to encounter online content and behaviour that is not age appropriate for them, and which is often harmful and even illegal. Our research has found that this has become a normalised part of a child's online experience.

> **I know most people lie about their age but they do that because there is a rule. If they don't make a rule about how old you need to be, people wouldn't have to lie..**
>
> **– 15 year old girl[10]**

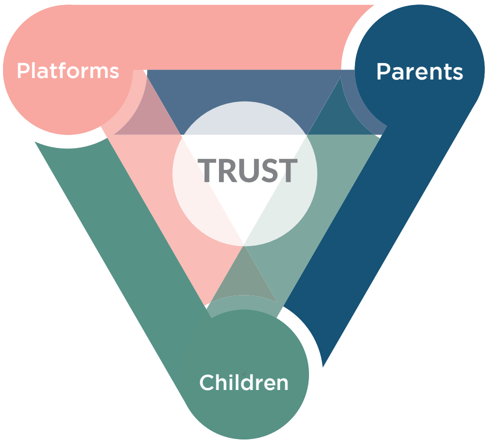
> **...I had my first account when I was about Year 4 or 5 .. I did have to lie about my age. I scrolled to 1901 and they let me on**
>
> **– 10 year old boy[11]**

Throughout VoCO engagements with children it was apparent that for them online harms are endemic to using the internet. During engagements, children were comfortable talking to experts about the fact that they had commonly been approached by adults they did not know, were familiar with bullying and with viewing upsetting content, and were very 'matter of fact' about their negative online experiences. However, these experiences did not translate to them as a reason to go 'offline' - they saw these experiences as an unavoidable part of their lives. Many, we found, want their parents to be an active part of their online safeguarding experience. **The VoCO engagements with younger children found that they view their digital parents as playing a key role in their online experience and want them to be actively involved in their online safety.**

Our research found that while digital parents consider themselves to have a key responsibility for keeping their children safe online, their ability to deliver this was - they felt

[7] Europol, 'Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic', 2020
[8] Express & Star, 'Girls as young as six sexting during pandemic, cyber safety research suggests', 2020
[9] Refer to page 47 reference #1
[10] Ibid
[11] Ibid

- limited by the current digital landscape, which was confusing and provided insufficient safeguards. Parents and carers expressed being aware of the dangers posed to their children by going online, but feeling disempowered by the current situation. During VoCO engagements 'digital parents'[12] described feeling trapped - having to choose between banning access and isolating their children from peers, or allowing access and risking harm. This tension was especially evident in the parenting of children in non-traditional care environments - for example, those in foster homes. These digital parents described struggling with the challenge of striking a balance between safety on the one hand and freedom and opportunities on the other. We found that these children were often most in need of safeguarding online and child safety measures such as age assurance. However, current approaches to age assurance have not considered how methods could disproportionately impact such children or other exclusionary factors in their use. An evidence base is needed here to enable the development of inclusionary methods.



The VoCO triangle showing the relationship between child, digital parent and platform

For digital parents to be engaged and empowered they must be part of the solution, informed on the options available to them and not overly burdened by the process.

Core to the insights from VoCO is that **children's internet safety relies upon the existence of trusted relationships between online platforms, children and digital parents.** Trust is highlighted here because it is the essential component to bringing about children's online safety.

During VoCO engagements both parents and children expressed a desire for platforms to do more to protect child users online. Our research found that just because children are not supposed to be on platforms it doesn't mean that they aren't. Industry participants acknowledged the importance of safeguarding users, and emphasised the importance they place on user safety, especially the safety of younger users. The process of recognising child users was, however, considered to be a complex ask. Platforms recognised the value of taking a risk-based approach to age assurance. Such an approach would require companies to assess the likelihood of children accessing their platform and the severity of risk posed to them, selecting an age assurance method that delivered the confidence that fitted this risk profile. For example, a site that contains age restricted products or services such as online gambling would want to have a high level of confidence about the accuracy of which of their users are under 18. This site may choose an age verification approach to deliver this. Industry stressed that currently they did not feel they had the detailed information needed to be able to make these assessments and implement age assurance effectively and with confidence. There is no consistent approach to defining risk across platforms or for establishing the corresponding level of confidence needed from an age assurance measure. Our research also found that the sharing of insights and best practice on age assurance is not commonplace amongst industry. During VoCO industry engagements platforms expressed the need for the development of a risk assessment to help guide their actions.

Platforms also had concerns over its impact on their liability and the commercial viability of implementing it. Platforms did not want to be commercially disadvantaged if competitors aren't also compelled to take the same steps to age assure users that they themselves are compelled to take. Platforms also wanted acknowledgement that no age assurance method could provide 100% accuracy, and that harm may still occur even with effective age assurance and differentiated services in place. If harms did occur, platforms wanted their actions to recognise child users and the subsequent safety features they put in place to be taken into consideration when they are being assessed for liability for harm.

The concepts, data and methods for age assurance.

The technical options for assessing the age of users online are broader than age verification. VoCO Phase 2 has explored the methods, data sources and approaches that can facilitate proportionate age assurance online.

[12] In the online environment, the parental responsibilities can extend to a range of individuals in a child's life, not just the biological parent. For this reason, when discussing the online environment, VoCO uses the term 'digital parent'.

Our research found that the data landscape for age assurance is promising, with sources either mature or maturing quickly and others that present opportunities for innovation. Our research assessed over 30 potential data sources for age assurance, which fall within three key areas: officially provided, user provided and automatically generated.[13] The project developed a framework to help bring clarity to the data and map out considerations for use, including accuracy. We found that currently the data sources VoCO looked at provide varying levels of confidence for age assurance - for example, an officially provided data source such as a passport will provide a different level of certainty to an automatically generated data source such as a user's use of language. Our research found that applying statistical methods to combine age assurance methods could enhance the level of age confidence over time. The diversity in data sources and their maturity levels highlights that this is a fast-moving field which could, with greater access to data sets and investment, provide further opportunities for accurate age assurance.

To be widely used, age assurance needs to be an easy and safe experience for the user. VoCO Phase 2 considered the user experience and data protection implications of approaches. The project ran a technical trial that aimed to scale age assurance while preserving data protection. The benefit of such an approach being that multiple stakeholders across different parts of the digital ecosystem can age assure a user with the same information, reducing friction for users and the sharing of personal data. This means that if a child has had their age band established once, this could enable age assurance across multiple platforms without parents needing to repeatedly consent to the further sharing of data. A trial of this process was run as part of Phase 2 and found that it was a viable approach. Further trials are recommended and greater work needed to explore how trust between the participants can be assured at scale, through a structure like a Trust Framework or a similar approach.

The landscapes and incentives for VoCO

VoCO Phase 2 looked at what landscape and incentives are needed to bring about the VoCO vision and drive the large-scale use of age assurance.

During VoCO engagements with industry it had been stressed that industry needed best practice examples to guide their implementation of age assurance and child safety efforts. In response to this the project undertook a review of current technical, legal and policy standards and frameworks that relate to the protection of children online and the security of their data and mapped these against VoCO's aims. Our research concluded that while many relevant standards and frameworks exist none on their own would enable the VoCO Manifesto[14] in full. There were, however, many high impact measures identified. The work mapped this into a template VoCO standard which, if implemented by organisations, would help them fulfil the VoCO Manifesto and deliver a higher safety level for children.

For age assurance to be widespread it is likely that regulation will be needed in the wider child online safety space to incentivise its adoption. VoCO Phase 2 engaged with domestic and international regulators and industry to look at what considerations this might raise. Throughout engagements it was stressed that the dynamic nature of the online environment was an important consideration. Regulators and industry emphasised the importance of proportionate, risk-based and technology agnostic regulation that would stay abreast of technical developments, while providing flexibility and space for innovation. It was felt that a prescriptive approach that mandated a specific technology or method of age assurance risked exacerbating the current challenge of children lying about their age. For example by resulting in overly heavy measures being used that either excluded some users due to the need for specific documents or encouraged children to circumvent the system.

Our Recommendations

Our vision is one where children are incentivised to be honest about their age, and platforms tailor their products and services to ensure child users have a safe experience. From our engagements and research we have developed a Manifesto for Change [pg 10] that sets out the relationship between child users, digital parents and platforms. We want a relationship of trust and mutual benefit between children and platforms to be 'the norm'. This requires innovative collaboration between platforms, age assurance providers, data source authorities and regulators. Users, in particular children, must have **trust** in the process.

[13] Refer to page 47 reference #5

[14] Please refer to the VoCO Manifesto on page 10

To help make this a reality we recommend the following action is taken in the key areas:

1 *A regulatory strategy for age assurance*

The successful realisation of the VoCO Manifesto requires regulatory involvement. This does not mean mandating age assurance. To enable a regulatory landscape that incentivises platforms to actively recognise their child users, incentivises children to be honest about their age and encourages growth and innovation in the age assurance market, **we recommend:**

a. Undertaking research on the risks posed to children by online services, to help inform the proportionate and risk-based use of age assurance. This research should engage with industry and subject experts.

b. Taking action to secure regulatory alignment between relevant current and emerging regulatory frameworks. A 'task force' of government and relevant regulators would help to deliver this.

2 *Encouraging industry's adoption of age assurance*

For platforms to adopt age assurance they need to have confidence that the action they are taking is appropriate, enables greater safety for their users and does not impair the user experience. **We recommend:**

a. Developing industry benchmarks, facilitated through research on the risks posed to children by online services. This research should engage with industry, regulators and subject experts.

b. Developing best practice examples, in partnership with regulators and industry.

3 *Stimulating innovation in the age assurance market*

There is a growing market for age assurance. Innovation is needed to ensure a diverse range of platforms and users' needs are met. **We recommend:**

a. Taking action to promote the age assurance market among industry and users.

b. Supporting the development of industry standards to ensure consistency and trust in age assurance solutions.

c. Exploring accessibility to testing data, to improve accuracy in age assurance methods. This is particularly important for methods that rely on training an algorithm, such as age estimation based on biometric data.

d. Taking action within the engineering and design community to ensure that age assurance is considered as part of voluntary design codes of practice.

4 *Growing public confidence in age assurance*

For age assurance to be effective it needs to be widely used. For this to happen digital parents and children need to have confidence and trust in it. **We recommend:**

a. Undertaking research into how age assurance may disproportionately impact on some children and explore how these insights can be reflected in the development and implementation of age assurance.

b. Supporting digital parents to gain a better understanding of the safeguards that age assurance offers, and the compliance action taken by providers and platforms.

Index

Please note: All references can be found in Appendix 5 and the supporting documentation and media referenced in this report is available on request dependant on classifications, security clearances and any IP or confidentiality rights. Please send related requests to: sso@vivace.tech. There is also a glossary of terms in Appendix 6.

1. VoCO Phase 2 - Our Objectives and Approach

The first phase of VoCO brought together government, industry, charities, legal experts, technologists, child protection specialists, and data protection specialists to test the VoCO hypothesis from multiple angles. The consensus was that the VoCO hypothesis is achievable and can address the core challenges that currently undermine children's online safety.

It was recognised that, by implementing age assurance, platforms would be better positioned to recognise their child users and therefore be able to adapt their online spaces to provide a higher level of safeguarding to those that need it.

VoCO Phase 2 has set out to build on phase one and test the practicalities and feasibility of age assurance. Our objectives were to:

1. **Capture the interests of children and their digital parents, and the incentives for industry,** through cross-sector engagement involving children, digital parents, industry experts and policy makers, and create a **'Manifesto for Change'.**
2. **Describe age assurance and introduce the new concepts, systems and policies required to implement it in today's landscape.**
3. **Define the necessary drivers required to make VoCO a reality.**
4. **Explore and bring to life ideal 'VoCO futures',** exploring how age assurance could practically make children safer online in the future.

To achieve these objectives Phase 2 commissioned seven workstreams and engaged with a broad range of stakeholders. Each workstream produced a report, these are referenced below and can be requested from ACE:

'Child's Voice' engagements

Engagement with children across a range of ages and backgrounds was carried out to provide an understanding of the current lived experience for children and young people online. Parents, teachers and carers were also interviewed to understand their role in safeguarding children and how age assurance might affect current dynamics.[15]

Industry engagement

We worked with representatives from across industry including app providers, service providers, and adjacent sectors to explore the VoCO Manifesto, obtain initial reactions and understand how solutions might be implemented, informed by a risk-based approach.[16]

[15] Please refer to page 47, reference #1
[16] Please refer to page 47, reference #2

Regulators

We explored how regulators and other bodies in the UK and overseas approach online regulation and what their views of online age assurance are in the context of making children safer online.[17]

Standards

Through the review of existing standards and frameworks, the focus of this workstream was to outline a 'template standard' that could facilitate the VoCO manifesto and allow it to operate at scale.[18]

Data Sources

To understand the macrocosm of potential age assurance data sources and how they could be put to use. This workstream focused on developing a taxonomy of data sources, which included assessments of the feasibility of the types of data sources identified, based on a range of criteria such as technical and legal feasibility.[19]

Commercial Models

Commercial viability is an important consideration when implementing age assurance methods. This workstream explored the commercial models that could potentially support emerging architectures, with pros and cons listed for each, as well as likely significant cost bearers.[20]

End-to-end proof-of-concept

To bring VoCO into reality, we carried out a proof-of-concept to demonstrate how platforms can recognise child users by age band. This was a cooperation between four commercial companies including a major global player.[21] Alongside this trial we also conducted research into several other age assurance solutions to understand the landscape of different solutions in development.

[17] Please refer to page 48, reference #3
[18] Please refer to page 48, reference #4
[19] Please refer to page 48, reference #5
[20] Please refer to page 48, reference #6
[21] Please refer to page 48, reference #7

1.1 Phase 2 Engagement in Stats

18 children
In years 5 and 6

16 children
aged 12-15 in an **independent day school**

15 children
in the **care system**

9 children
aged 14-15 in **mainstream comprehensive school**

22
parents or carers

2
teachers

4
core UK regulators

3
parallel regulators

6
overseas regulators

7
industry bodies with quasi regulatory roles

4
unregulated areas of emerging technology

40+
standards and frameworks reviewed

30+
Age Assurance data sources analysed and assessed

3
cross-sector and government workshops hosted by ACE

3
industry roundtables

2. A Manifesto for Change

Our vision

VoCO Phase 2 has aimed to clarify the concepts and processes that surround age assurance and outline the frameworks, collaboration and action needed for an internet that actively recognises children and adapts the spaces they use to make them safe.

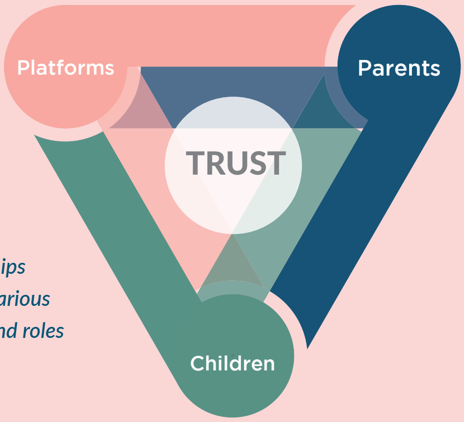
Our vision is that by actively recognising their child users, platforms create a positive sense of security and opportunity online. Age assurance should not be a tool to create a 'walled garden' effect where children are isolated or confined into a reduced version of the internet. Key to this is a relationship of trust between Platforms, Digital Parents and Children.

To help support this we have developed Manifesto for Change that sets out the principles underpinning the relationship between children, digital parents and platforms that would facilitate VoCO. These principles were developed through engagements with platforms, digital parents and children, as well as research activity and the Phase 2 workshops. They are not intended to be considered as final. Appendix 4 sets out the evidence gathered to create this manifesto.

VoCO Aims

"…. to bring about an internet that actively recognises children and adapts the spaces they use to make them safer by design"

Platforms	Digital Parents	Children
recognise which of their users are children and design appealing age-appropriate services for them that meet their needs and safeguard them from harm.	feel empowered to protect their children online because they have a good relationship with the platforms their children use.	are not compelled to lie about their age online because platforms that appeal to them and their friends actively identify and cater for them.



The VoCO triangle illustrates these key relationships and provides a framework to consider all of the various technologies, protocols, processes, information and roles necessary to achieve it.

VoCO Principles

Platforms

As a platform, if I'm going to recognise and protect my child users...

I want a clear understanding of the risks they face on my platform, and the practical measures required of me to protect them

I don't want to be commercially disadvantaged because my competitors aren't held to the same standard

I want my liability to recognise the measures I have implemented to protect them if, despite these, harm still occurs

Digital Parents

As a digital parent, if I'm going to allow my child to use your platform...

I want peace of mind that the platforms are protecting my child and they are giving me the information I need to do the same

I do not want it to be burdensome because I need to make timely and informed decisions about my child's wellbeing

I want to know my child's rights are being respected as a result of the decisions taken by the platforms and myself

Children

As a child, if I am going to be honest about my age...

I do not want to feel like I am missing out because my friends can do things that I cannot

I want a better experience that lets me do more rather than less things

I want to feel safer because I know I am being protected from the bad stuff that can happen online

3. Age Assurance - Concepts and Components

Options for assessing the age of users online are much broader than age verification. VoCO has explored the methods, data sources and approaches that can facilitate proportionate age assurance online. This chapter summarises that work.

When assessing whether age assurance is beneficial for a child's safety, our research found that establishing the likelihood of children accessing the platform and understanding the potential risk posed to a child are essential. Our research found that just because children are not supposed to be using a platform does not mean they aren't. Platforms should be encouraged to assess and record the likely number of child users on their sites, and take steps to establish the degree of risk posed to them by the platform. During VoCO engagements industry highlighted that currently they do not always have the necessary details or shared understanding of risks to confidently make these assessments.

In implementing age assurance VoCO found that there are a broad range of methods available to companies, which we have grouped into 10 primary approaches. These can be facilitated by a variety of data sources which we have mapped under three primary categories: officially provided; user reported; and automatically generated. To help bring greater clarity to this data landscape VoCO has mapped these sources into a framework, the Data Source Type Taxonomy (DSTT), which considers factors including reliability, costs and the legal implications of using the data. VoCO found that the data landscape was promising, with mature data sources already being used for age assurance purposes and many that are rapidly maturing or present promise for innovation and growth.

This chapter also discusses scaling age assurance. Achieving this is commercially desirable and from a user experience position too, as it reduces the number of times a user and platform is required to re-share personal data. In chapter 4 we discuss the technical trial run on this approach in VoCO.

3.1 What is Age Assurance and When is it Beneficial?

Age is the single universally recognised attribute that separates children from adults, it is therefore an important metric to direct online protection efforts. Although vulnerability is exclusive to every individual, and not always shaped by age. Due to their development needs children and young people are uniquely vulnerable online and offline compared to the majority of adults.

How does age assurance differ from age verification?

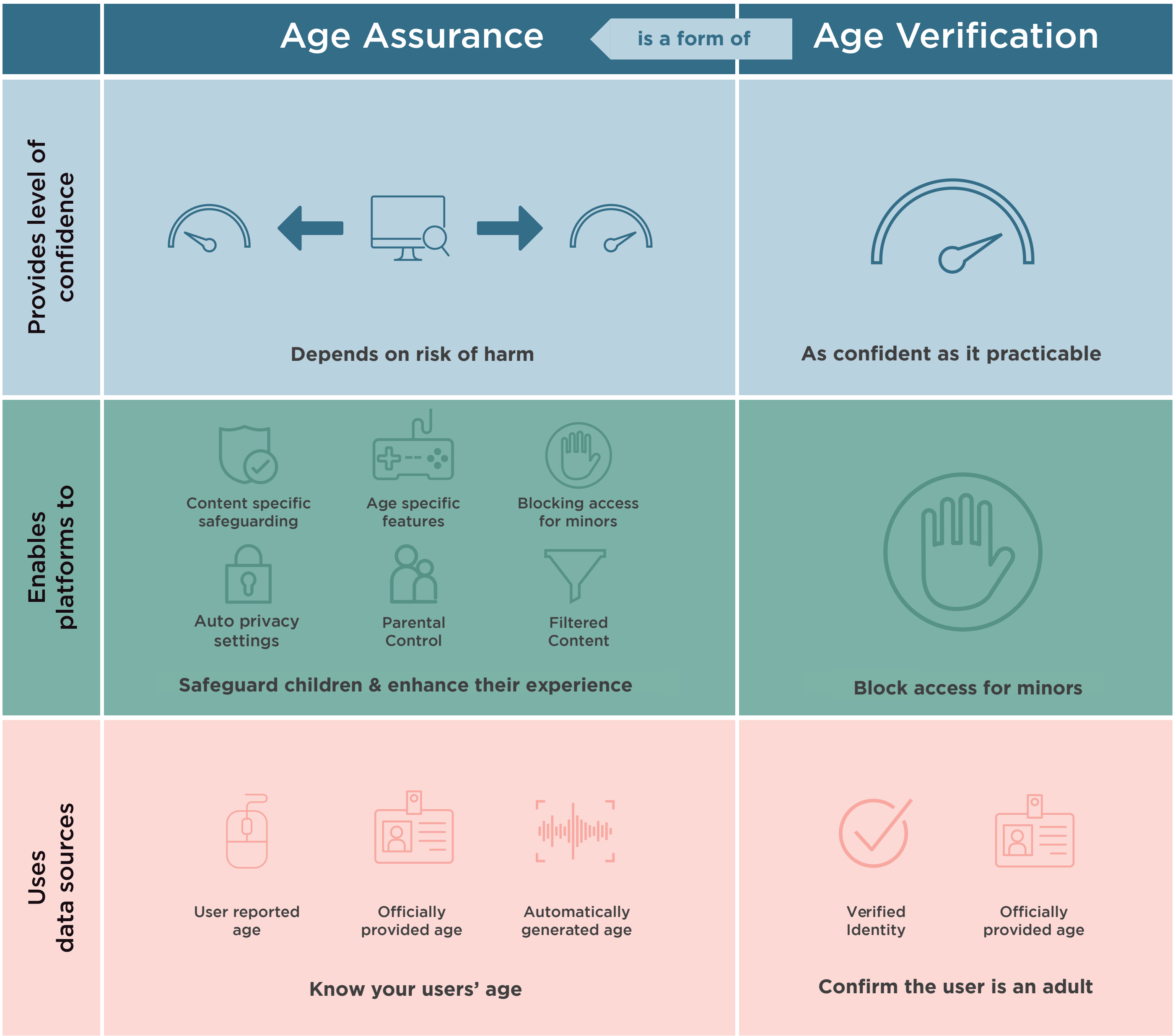
The development of the concept and definition of age assurance has been an important output of VoCO. **Age assurance is the broad term given to the spectrum of methods that can be used to assure a user's age online. Age assurance allows companies and users to jointly choose from a range of measures that are suited to the specific risks and service needs.**

Much discussion on recognising children online has centred around age verification. Age verification is a form of age assurance where a user's age is established through a full identity verification process to a high level of confidence. There are some situations where using age verification may be the most suitable solution for a platform. Currently, age verification is most commonly used to help businesses meet legislative requirements concerning age-restricted products and services by restricting access to users who cannot provide officially held evidence that they are over 18 years of age.

Age verification relies on establishing age by determining an individual's identity and using that knowledge to access officially held data which confirms their age. It is not, however, a panacea. The age verification ecosystem is geared up to identify adults (age 18+) rather than discriminate between children in different age bands to better support their needs. The data sources that age verification methods rely on, for example a passport or credit card, often encourage businesses to apply an 'all or nothing' approach that blocks users who are incapable of providing officially held evidence that they satisfy the legislative age threshold. This risks excluding users who meet an age threshold but do not possess the right data to prove this.

Acknowledging the breadth of options available to age assure users including but not limited to age verification is important for enabling an approach that is both proportionate and effective at protecting children online.

The table below illustrates pictorially the differences between age assurance and age verification when a platform is for 18+ users only:



	Age Assurance	is a form of Age Verification
Provides level of confidence	Depends on risk of harm	As confident as it practicable
Enables platforms to	Content specific safeguarding Age specific features Blocking access for minors Auto privacy settings Parental Control Filtered Content Safeguard children & enhance their experience	Block access for minors
Uses data sources	User reported age Officially provided age Automatically generated age Know your users' age	Verified Identity Officially provided age Confirm the user is an adult

When might age assurance be beneficial?

There will be circumstances where a platform does not need to establish a user's specific age but their age band (e.g. 10-12) is sufficient. The ICO Age Appropriate Design Code provides a list of recommended age bands based on children's level of development.[22] As such the use of 'age' in this section should be taken to mean 'age band'.

Our research suggests that if a platform presents a high risk of harm to children it would be beneficial to use an age assurance measure that gives a greater level of confidence in the age of the user.

By having this information platforms are then able to implement appropriate safeguarding measures, rather than blocking the child. We found that platforms which are inherently safe due to their design, features and/or content (such as child-directed sites) can use age assurance as a way of further enhancing the child's online experience and tailoring the content to their age band.

Age assurance encompasses a broad range of measures to establish a user's age. These include self-declaration, confirmation by digital parents and peers, automated analyses performed by online platforms, and the identity related checks which have traditionally been employed to verify age.

VoCO found that where platforms posed a potential risk for child users age assurance was an important tool for risk mitigation. Assessing risk means in practice establishing two things:

a **That children are likely to be using the platform, and**

b **The platform has been assessed as posing a defined level of risk to a child.**

We expand on these areas in the next sections.

3.2 Establishing the Likelihood of Children Accessing a Platform

Our research found that it was common for children to lie about their age to gain access to platforms that appeal to them. Just because a platform's intended audience is not children does not mean it won't have child users. A platform can assess the likelihood that it has child users based on several factors: this could be ascertained through a combination of self-assessment and external independent assessments. Examples of these factors could include:

- Independent surveys of platform users.
- Assessment of platform content features against likely target audience.
- Transparency reporting from the platform, including advertising metrics where age is a factor.

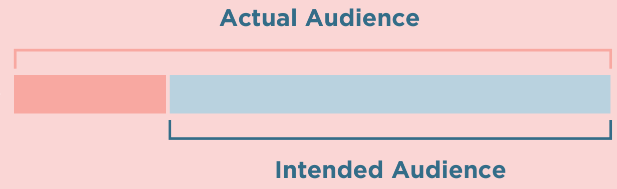
In assessing the age of users, platforms could choose one or more methods that suit their specific service and are appropriate to the risks posed. Different methods may rely on different sources of data, which may have different privacy implications and cost models (further detail on potential data sources is included in Section 4: Bringing VoCO into reality). Generally data protections must be considered when determining the best approach to age assurance.

It is important that platforms are incentivised to accurately record their 'actual user base' demographic, rather than their 'intended user base', i.e. those that are above the minimum age set out in their terms and conditions. Just because children shouldn't be on a platform doesn't mean they aren't actually there.

[22] Information Commissioner's Office (ICO), 'Age Appropriate Design: A Code of Practice for Online Services,' 2019. (NIST SP 800-63b)

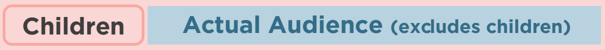
Actual vs. intended audience in the current environment, compared to VoCO vision

Current Situation:
Platforms have a minimum age policy but have very limited checks to prevent access to underage users. For example, many sites require users to check a box stating they are over 13, or to select a date of birth, without any additional checks to verify this information.

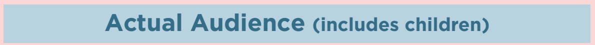


VoCO vision for future:
Platforms effectively assess their actual audience (based on a number of factors).[23] If children are likely to be users then one of the following options is applied:

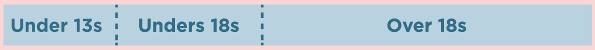
a. The platform is known to be unsuitable for child users. Age assurance is therefore used to identify and block underage users.



b. Age assurance is used to assess the likely youngest age of users. The whole platform is found to be age-appropriate for the youngest likely users.



c. The platform has varying degrees of suitability for different age bands. Age assurance is therefore used to identify younger users and provide them with age appropriate features and content.



3.3 Establishing the Level of Risk to a Child on a Platform

The risk that the platform presents to children is influenced by several factors, including:

- platform architecture and design (including processing of personal data)
- platform operation (including moderation)
- nature of content shared on the platform
- the makeup and behaviour of its user base

Through the course of Phase 2, we engaged with industry to understand what they would require in order to accurately establish the risk of their platforms. Although these were very early stage discussions, the necessary elements included:

- Consistent definitions of threats/potential harms and agreement on the risk level posed by specific service features
- Agreement on the likelihood of the threat posed to children in given scenarios
- Agreement on the best options for risk mitigation

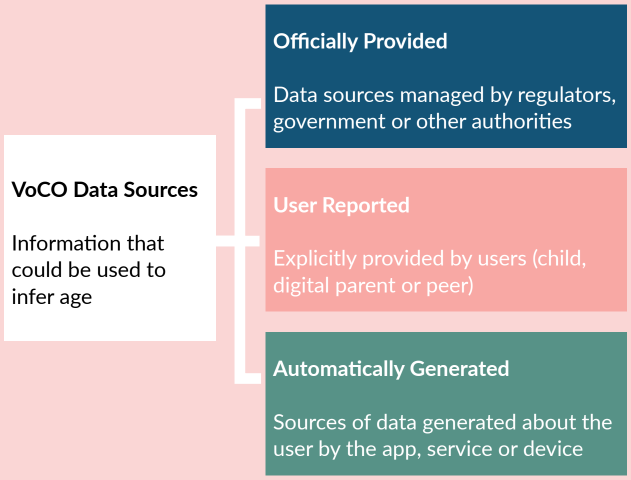
During VoCO industry engagements, industry shared that they currently felt these elements were lacking and limited their efforts to protect children online. They described an agreed risk assessment with risk case studies as an essential component to help them confidently identify and mitigate risk.

[23] The ICO's Age Appropriate Design Code [18] will also place a requirement on companies in scope to undertake an assessment of their actual user base.

3.4 Obtaining Data for Age Assurance

Being able to perform age assurance is dependent on the effective use and application of age-related data sources. When choosing a data source it is important that organisations consider regulatory data protection obligations and the risks to these presented by different approaches, and take steps to mitigate these.

Phase 2 considered the current macrocosm of data sources, the methods of application and the implications for age checking. There are three primary categories of data sources for age assurance: officially provided; user reported; and automatically generated. These data sources can be deployed to provide age assurance via 10 primary methods - which are detailed in section 3.5 below.


VoCO Data Sources
Information that could be used to infer age
Officially Provided
Data sources managed by regulators, government or other authorities
User Reported
Explicitly provided by users (child, digital parent or peer)
Automatically Generated
Sources of data generated about the user by the app, service or device

Data Source Type Taxonomy (DSTT) Structure

An output of VoCO Phase 2 has been to develop a structure to classify and assess the effectiveness of different sources - the Data Source Type Taxonomy (DSTT)[24] and bring clarity to this landscape. This structure is designed to support a better understanding of the current data sources that are available to platforms and users which could be used to deliver effective age assurance, including considerations for their use.

It is important to note that the different key actors in age assurance - the child, the digital parent and the platform - interact with the data sources in different ways. Children and digital parents primarily provide 'User Reported' age data, for example data generated by the digital parent or child, such as date of birth. They are also the subject of 'Officially Provided' data and the target of collection for 'Automatically Generated' data sources. On the other side of this exchange, platforms are the potential recipient or collector of all three of the data sources contained within the DSTT and will use these to carry out their assurance function.

The table on the next page outlines, at a high-level, the DSTT we developed. It should be noted that this is a high-level capture with edited examples and considerations. Data sources mature and their considerations for use change. As such, the DSTT is intended to be a living document.

A comprehensive assessment of this work is included in a 'Data Sources Report', which was produced for VoCO Phase 2 and is available on request.[25]

[24] Please refer to page 48, reference #5
[25] Ibid

Source	*Generator*	*Description*	*Example*	*Considerations*
Officially Provided	Large Central Databases	Data accessible through discrete, official databases, which are managed at a national level by central government or agencies.	Passports, Visas, & Electoral register	High confidence verifying an individual's age where they engaged with a govt. agency. However potential disadvantages elements of society who aren't represented in Govt. databases. High cost to maintain accuracy, coherence and security. Statuatory restrictions apply to data use.
	Distributed Information	More dispersed, less structured data sources, equally authoritative but might require significant resource, human or otherwise, to support the synthesis and supply of data.	Medical Records	Authoritative. However, may require significant resources (human or otherwise) to support the synthesis and supply of data.
User Reported	Digital parent provided	Data generated or provided by the digital parent of the potential child user, who in turn may be required to verify themselves.	Financial consent for online purchases & School enabled access	Trust in the data is only as good as trust in the parent. May also cause administratrive and technical burden for the parent. Delays may cause users friction.
	Child provided	Data generated or provided by the potential child user.	Account handles	Children (and adults) may lie about their age to gain access to age restricted platforms. Minimising friction is essential to an effective industry response.
	Peer provided	Data provided by other (trusted) users of the app, service or platform, who have some presumed social relationship with the potential child user and can effectively vouch for their credentials.	Peer based attestation	Delays cause user friction and may impact experience. Peers need to vouch for their credentials which introduces reliability. Validation could include other age assurance data sources to enhance accuracy such as online behaviour analysis.
Automatically Generated	Body metrics	Data derived by the user's physical movements or interactions with a device.	Haptics (touch data) & Gait / Motion analysis	Experimental data source. Delivers minimal friction. Would need to be combined with other age assurance data to enhance accuracy.
	Environmental	Data derived from the physical or infrastructure environment in which the user is based.	Technology Environment & Audio Environment	Experimental data source. Delivers minimal friction. Would need to be combined with other age assurance data to enhance accuracy. Could provide additional information about user risk due to setting.
	Behavioural	Data generated by the users while using an app, service or platform.	Social Network data & Pattern of app / platform use	Maturing data source. Delivers minimal user friction. Needs to be combined with other data sources to enhance accuracy.
	Biometrics	Data derived from static (or long-term) physical characteristics of the user.	Facial Morphotype	A range of maturity depending on data type. Delivers minimal user friction. Potential for high accuracy. Some public perception concerns over autonymity / privacy concerns might impact user adoption.

Data Source Type Taxonomy (DSTT)

3.5 Methods for Age Assurance

Platforms can use the data sources, outlined in the previous section to age assure their users. In practice, there are 10 broad methods for assessing the age of a user, which are listed in the box below.

These methods can be applied singularly or in combination to deal with different age assurance needs or use cases. For example, for a platform that needs a medium level of confidence, a user could initially declare their age as part of the onboarding process, and alongside this an automated age assurance method (such as using AI analysis) could be used to confirm the declared age. If this measure suggests a different age band than that stated, which reduces confidence in the initial assessment, a request could be made to validate the user's age through a verified digital parent. In this example, the platform has applied a range of methods (which draw upon a variety of data sources) to achieve the required level of confidence.

As an online platform I have increased my confidence in your age because:

1. You have **declared** your age.
2. I know your **digital parent** and they have declared or confirmed your age.
3. A **trusted online provider** has authenticated your age.
4. I have contacted individuals in your **peer group** and one or more of them have confirmed your age.
5. You have provided **hard evidence**, from an official source, that enables me to confirm your age.
6. I know your **identity** and have used this to confirm your age from trusted sources.
7. Your **physical characteristics** indicate your age or are consistent with your declared age.
8. The way that you use your **body** to interact online indicates your age or is consistent with your declared age.
9. Your **behaviour** online indicates your age or is consistent with your declared age.
10. Your location and physical or infrastructure **environment** indicates your age or is consistent with your declared age.

Methods for age assurance

3.6 Defining Levels of Age Confidence for Platforms

Age confidence is a measure which determines how certain a platform is about the age of their individual users. The age confidence level needed by a platform is based on the assessment the platform has made on the degree of risk posed to a child by the service. For example, if they have assessed that there is a high likelihood of harm occurring to a child on their service they will require an age assurance method that provides a high age confidence level. By doing so the platform can be reassured that it is using a method that tells them to a high degree of accuracy which of their users are children.

It is important that industry is able to have a clear and consistent approach to securing age confidence levels in a way that can be independently verified. Currently, data sources provide varying levels of confidence. As with age checks in the offline world it is not possible to have 100% confidence about a user's age online; approaches can be gamed or undermined given sufficient resources or technological sophistication. Which is why improving confidence in the accuracy of an assessment is important. It is possible to improve confidence by combining multiple sources of data. Applying statistical methods allows for an incremental approach to enhance user age estimation certainty over time. It is important to note that combination is not the sum of its parts. Dependence between data sources cannot be ignored, and further experimentation with real data is required to estimate and account for the impact of these dependencies on age confidence.

It is also important to remember that confidence in any given age assurance method is increased if children are not incentivised to lie about their age and game the system. The ideal scenario is one where children are incentivised to be honest. To make such a relationship between children and platforms 'normal' will require innovation and collaboration between platforms, age assurance providers, data source authorities, future regulators, and of course users - particularly children. It may also mean that the way in which an age confidence level is achieved will differ platform to platform.

For age assurance to be effective, once a platform's level of risk to child safety has been established, it is important to define the level of confidence that a platform is required to have about the age (band) of its users - platforms will demand clear definitions of risk to enable them to determine which age assurance measures they need to apply. To inform ongoing research into effective definitions for levels of age confidence to apply to different age assurance methods the following draft definitions have been produced as part of VoCO Phase 2:

High confidence: Where a platform has been defined as posing a high likelihood of risk to child users the platform is required to have a high level of certainty that the person accessing their service is the age they say they are, because the age of their digital identity is verifiable.

Moderate confidence: Where a platform has been defined as posing a moderate likelihood of risk to child users the platform is required to have a medium level of certainty that the person accessing their service is the age they say they are. However, there are likely to be inconsistencies in the answers given between methods used to verify age.

Low confidence: Where a platform has been defined as posing a low likelihood of risk to child users the platform is required to have limited-to-no certainty that the person accessing their service is the age they say they are.

The following table sets out some of the relevant factors that could be used to measure levels of age confidence that a platform has for its individual users.

	High [confident]	*Medium [moderate]*	*Low [unsure]*
Type of data source(s) used to assure age	Rated as providing a high level of certainty E.g. obtained from validated officially held records such as a passport	Rated as providing a medium level of certainty E.g. obtained from behavioural data such as from multiple access attempts	Rated as providing a low level of certainty E.g. 'tick-box' or self-assertion
Combination of data points used to assure age	Agree on a given age band e.g. <13, 13-16, >16	There is some ambiguity on the age band	Do not agree on age band or no attempt made
Use of accredited Age Check Data Providers	All sources use accredited age check providers (which can be evidenced) Use by default/comprehensively	Few sources use accredited age check providers Use is limited	No sources use accredited age check providers Not used

Factors in measuring age confidence

3.7 Age Checking and Scaling Age Assurance

Age Checking

Age checking is the means of establishing age, as a single attribute, without the need to collect any additional personal data (such as name, address and date of birth). Age checking reduces the query to 'Is this user between the age of 13 – 17?' Meaning that a yes / no response can be passed in the form of an 'Attribute Token'.

Attribute Token – *A token which is stored and passed in a digital form, and can carry only the attributes (e.g. age, or age band) that a user is required to provide to the requesting service or platform. This is called tokenised age checking.*

Conceptually, this is the same as a young person producing their 'young person's railcard' when buying a ticket at a train station. The card doesn't contain a DOB or personal address but does have a photo and an official hologram. In the rail card example, the ticket seller is able to establish that this is an approved token indicating the customer is under 17, and that this customer is the owner of the token.

PAS1296:2018 is currently the industry best practice for online age checking. It focuses on the reliability of the check as well as enabling businesses to consider data minimisation and acting in a privacy preserving way (as required by the GDPR).

Trust is an essential aspect of age Checking. PAS1296:2018 considers the level of assurance that the person associated with the age check is in fact the person to which the age check was performed, plus the reliability in the processes leading up to and including the authentication process itself.

Age checking is of interest to VoCO because it it is not limited to officially-provided data sources and it provides a means for Age Check Providers to undertake age assurance in a way that only determines and shares the age attribute. Our research showed that children are concerned about their personal data security when going online. Age checking is an important element to help provide reassurance that their data is being protected and anonymised.[26]

To understand more about how Age checking works and the key components involved you can read the British Standard Institute's PAS1296:2018 here (of note, payment required).[27] However, it should be noted that, for the purposes of bringing about the VoCO Manifesto in full, the scope of the PAS' guidelines should be updated. You can also visit the Age Check Certification Scheme website here for more information on Age checking and its related concepts.

Age Check Exchanges

As set out in the VoCO Manifesto, it is important that age assurance doesn't put an undue burden on children and parents to respond to countless data requests from multiple platforms. The VoCO Manifesto envisions age assurance as being frictionless, transparent and providing users with real choice about how it is achieved.

PAS1296:2018 also introduced the concept of Age Check Exchanges, which act as central gateways for multiple age check providers and platforms (known as relying parties[28]) to share age-checked tokenised attributes that meet established requirements for quality and reliability.

For a platform to use an Age Check Exchange, it would require them to sign up to a set of rules which are defined in a Trust Framework. A Trust Framework is the underlying structure of standards, rules, rights and responsibilities governing the operation of a digital identity ecosystem. It is an agreement between the participants - usually a digital identity ecosystem, but in the VoCO context an age-assurance ecosystem based on existing industry standards, policies and legislation - and is a means of achieving large scale trust online. It defines the rights and responsibilities of participants, specifies the rules that govern their participation, and outlines the processes and procedures to provide assurance to the other participating parties. The New Zealand government is developing a Trust Framework to support Digital Identity Services, and the US National Institute of Standards and Technology (NIST) has developed guidance on developing a Trust Framework for a digital identity ecosystem.[29, 30]

[26] Please refer to page 47, reference #1

[27] BSI PAS 1296:2018 https://shop.bsigroup.com/ProductDetail?pid=000000000030328409

[28] Online services operating within an age assurance ecosystem are known as relying parties. They are organisations that offer services, applications, and information that require restricted access.

[29] New Zealand Government 'Digital Identity Trust Framework', 2019

[30] NIST Internal Report, 'Developing Trust Frameworks to Support Identity Federations', 2018, (NISTIR) 8149

4. Bringing VoCO Into Reality

VoCO looked at what landscape was needed to bring about the VoCO Manifesto. This chapter looks at the structures and incentives that are needed for organisations to actively recognise their child users and create safer online environments for them. The project reviewed existing frameworks and standards that touch on the aims of VoCO to understand what current guidelines existed for organisations and where there may be gaps. While the research concluded there was no one existing standard that could enable the VoCO Manifesto it did identify the actions that could have the most impact. From these we have drafted a template VoCO standard.

Our research found that in addition to voluntary action it was likely that regulation will be an important incentive to encourage a VoCO approach and drive the use of age assurance. In VoCO engagements with domestic and international regulators the importance of considering the dynamic environment of the internet was emphasised. Regulators and industry emphasised the importance of proportionate, technology agnostic regulation that would stay abreast of technical developments, while providing flexibility and space for innovation. Industry also stressed the importance of coherence across the regulatory landscape to help support compliance.

As well as regulatory incentives the project also looked at the commercial considerations for actively recognising child users online. Our research found that for VoCO to be widely implemented the costs and incentives must be aligned - implementing a VoCO approach must be commercially feasible and the absence of doing so must be commercially untenable for an organisation. To enable this industry stressed the importance of creating a level playing field - no one wanted to be commercially disadvantaged by competitors not being held to the same standards.

The user's experience has been an important consideration during VoCO, including when assessing technical feasibility. We ran technical trials to explore how age assurance can be done in a way that reduces the burden on the user and is data privacy preserving. The results were promising. They showed that it was possible to scale age assurance across a range of services, providing a positive experience for the user while preserving the child's data.

4.1 Working Towards a 'Template Standard' for Age Assurance that is Desirable, Feasible and Practical

The standards workstream conducted a thorough review of current technical, legal and policy standards and frameworks related to the protection of children online and the security of their data. It compared them against the VoCO Manifesto aims and principles proposed in this report. This assessment identified numerous elements that are relevant to VoCO but found that no one standard or framework alone could enable VoCO.

Taking this into account, the standards team took insights from their assessment and discussed them with relevant stakeholders through a range of interviews and engagements (including industry and regulatory engagements, and the VoCO workshops). From these findings, we have developed a set of criteria, which has been refined and prioritised. These elements, the 'VoCO template standard', could be progressed in a range of ways - including voluntary action - for example industry standards. If acted on this template would help to bring about the VoCO Manifesto in full, with the 'high impact' criteria having the greatest effect on bringing about the VoCO Manifesto.

Impact of implementation on child safety	*Action*	*Description*
High	**Child Safety Impact Assessment**	A dedicated assessment should be performed by platforms of any service or changes to a service that impact the data or safety of children.
	Age confidence and regulation	Independent oversight may be required on platforms and age assurance technologies, especially where a high level of age confidence is needed.
	Platform certification (cyber)	Platforms should be required to undertake Cyber Accreditation in line with other standards such as ISO-27001.
	Parental dashboard	Works across platforms which enables parents to control and implement platform settings and is transparent so that the child knows it is supervised. Where suitable, individual tailored examples converging on best practice could be used.
	Risk assessment	Implemented for all platforms and provides guidance as to the content on the platform, setting out the functionality and what content is possible to access.
	Education	Continuing education is provided to the parent on the purchase of a device or content. Regulator-approved education material and links following approved guidelines should be provided through the platforms as a mandatory requirement.
	Safety settings	Standard settings for privacy, geolocation and security to be set by default for children requiring clear messaging and warnings if changes are made as to the implications.
	Privacy notices	Privacy notices should be easily accessible and in child-friendly, age range appropriate language.
Medium	**Platform trust (age range) mark**	All platforms should be required to display an appropriate age range for its content (at minimum <13, 13-18 and 18+). Recommend best practice ICO code • 0 - 5: pre-literate and early literacy • 6 - 9: core primary school years • 10-12: transition years • 13-15: early teens • 16-17: approaching adulthood
	Parental consent	A parental dashboard should provide progressive and flexible consent options.
	Reporting tools	Provide easily accessible reporting functionality to escalate concerns when online in addition to availability of offline guidance and support for the child.
	Incentivisation	Incentivisation to comply with the standard should be provided to platforms - economic, commercial, regulatory sanction or reputational. Incentivisation should be provided to the child in the form of positive 'nudges', for example access to additional content for providing high levels of age confidence.
	Sanctions	Sanctions should be actively implemented and communicated as one method of persuading platforms to adhere to the standard.

Low	**Payment records**	Process of payment for content by the parent should make it possible to identify on the credit (or debit card) statement the age band of the content (e.g. 18+) and act as a parental alert.
	Data / sandbox	Data held by platforms could be used to improve safety for children online. Consideration should be given to whether and how this can be accessed.

Standard criteria needed to bring about the VoCO Manifesto

4.2 Regulation and VoCO

Successfully implementing the VoCO Manifesto demands regulatory involvement. Two key requirements for a regulator in this space include the use of proportionate and risk-based regulation and capacity to address an evolving technical landscape.

The online space presents challenges for regulation. The ecosystem rapidly changes: new technology and platforms quickly emerge and scale, new opportunities are offered, but also new harms can quickly appear and put children at risk. Currently there are several existing regulators who have or will soon take on responsibilities in this area, including Ofcom, the Information Commissioner's Office, and the Gambling Commission.[31, 32, 33] Therefore, it will be important that there is alignment in the endeavours of each party, and open communication to avoid any contradictory efforts. The bringing together of a child online safety 'taskforce' or similar may be a way to achieve this alignment.

Proportionality and Innovation

The context surrounding risk - such as the technical capabilities of the platform, the likely exposure to children and the severity of the harm - need to be considered before choosing a method of mitigation. The response of the regulation (and indeed, the company) should be proportional based on assessment.

Any guidance on the appropriate application of age assurance will need to be risk-based and proportionate to ensure that children are protected from experiencing harm, while limiting any potential impacts on innovation and user's rights.

VoCO regulatory engagements found there are two elements of innovation as it applies to regulation:

- **The regulator should be innovative**, constantly monitoring social and technological changes to ensure the advice they give and the way they apply regulation is appropriate.
- **The regulator should encourage innovation in the industry** so that organisations look for innovative ways of complying with the spirit of any regulation.

> **eSafety's cyberbullying reporting schemes acts as a safety net for children who have been seriously cyberbullied. Our child-focused and victim-centric approach ensures that our investigators can look at the context of complaints and connect the complainant to relevant counselling and support services, work with social media services to have material removed, and engage with schools to resolve complaints where relevant. This cooperative model, alongside our powers to compel the removal of material, ensures that industry are driven to be proactive and reduces the need for us to issue formal notices to individuals.**
>
> **– Julia Fossi,**
> **Australian eSafety Commission[34]**

The cultural and technical landscape surrounding age assurance and online harms is rapidly evolving. To stay abreast of these changes, and ensure regulatory expectations remain relevant and effective, it is important that there is flexibility to accommodate new cultural norms, methods and technologies. As an example, the Video Standards Council (VSC) stays abreast of social changes by conducting regular research into what is acceptable in particular areas of video games - e.g. the degree and type of violence - to find out what the main public concerns are. Research takes place every 2 or 3 years.[35] Regulatory sandboxes have also been adopted by a number of regulators

[31] The revised Audiovisual Services Media Directive (AVMSD) will expand the Office for Communications (Ofcom) regulatory responsibility for audio-visual media content to video on demand and video streaming services.
[32] The ICO has regulatory responsibilities on data protection and data privacy through legislation including the GDPR and Data Protection Act.
[33] The gambling commission has regulatory responsibility for online gambling.
[34] Please refer to page 48, reference #3.
[35] Ibid

to encourage the development of compliant and innovative technologies. The Better Regulation Executive is currently working on a Guide to innovation and the regulatory cycle which describes an ‘innovation test’ designed to encourage evidence-based regulation that is flexible and takes advantage of innovation.

The approach to regulation can also encourage innovation. During VoCO engagements with regulators it was emphasised that overly prescriptive regulation carries the risk of restricting innovation. In contrast it was felt that regulation that is technologically agnostic and focused on outcomes, rather than mandating the specific technical steps a company should take, future proofs the regulation and encourages innovation from industry.

4.3 Commercial Incentives

Costs and incentives must be aligned such that implementation is not commercially infeasible, but makes non-compliance commercially untenable.

For age assurance solutions to be implemented, they need to be commercially viable. However, age assurance is not a single capability to which a charging model may be applied. The pros and cons of various potential charging mechanisms were considered as part of our research. We anticipate that VoCO will be integrated within a dynamic ecosystem and have varying market implications that factor in commercial incentives, cost drivers and dependencies on other parties. The table below illustrates the range of factors which are likely to be taken into consideration.

Commercial incentives	*Cost drivers*	*Dependencies*
Know my “user” demographic better and can tailor their experience / inform my market and commercial strategy more effectively Demonstrate my commitment to Corporate Social Responsibility Protect and enhance my brand value Reduce my corporate risk against legal liabilities Be more attractive to investors Attract more diverse and mainstream advertising revenue	Implementing technology that recognises users rather than devices Developing the ability for users to report, investigate and take appropriate action Monitoring / classifying content Child safety impact assessment	Platforms having a VoCO safety rating and design standard Standards developed, published and adopted Digital parents and children understand their risks and responsibilities to keep themselves safe online

Commercial Factors for Consideration

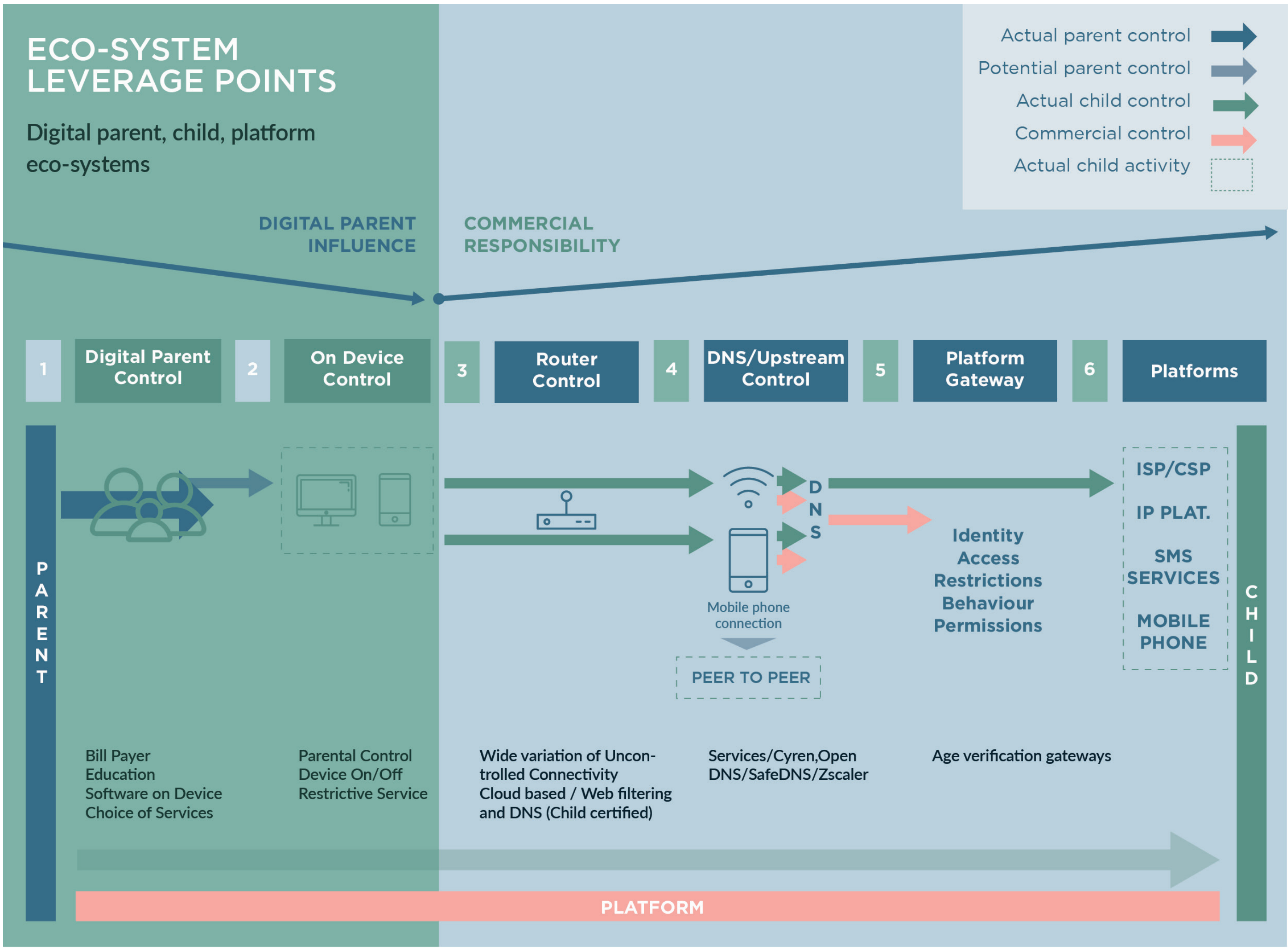
Our industry engagements showed that for age assurance to be widely used there is a need for a level playing field, where the same expectations or requirements are placed on all similar companies. In any implementation of VoCO, there is a cost which will need to be met by one or more entities. Furthermore, for VoCO to be successful, that cost must not be untenable for any one such body. At the same time, the impact of not implementing an age assurance approach must be sufficient that platforms and bearers cannot afford not to do so. As regulation is developed and implemented, there may be an opportunity to leverage consumer demand for platforms that recognise and safeguard children. Our VoCO engagements with parents suggested users might be willing to base their use of services on whether they are seen to have adopted appropriate social and ethical behaviours.

4.4 End-to-end Proof of Concept

Testing of an age check solution with children and their digital parents show that age assurance solutions could be both feasible and implementable.

As part of VoCO Phase 1, a start-up specialising in age checking (see section 3.7) ran a number of small-scale User Acceptance Testing (UAT) trials.[36] The findings from the initial trials of the previous VoCO commission indicated that end users' experiences were positive, but that further testing was recommended. Further testing should involve trials with one or more wider partners as well as the continuation of product market fit and scalability testing. Therefore, in parallel with the development of VoCO Manifesto principles to help enable the VoCO Manifesto, VoCO Phase 2 ran a workstream that continued to explore technical solutions. This extended trials of an age checking solution with children and their digital parents in the form of an end-to-end proof-of-concept (E2E PoC). It also involved further research and interviews with other age assurance providers.

The E2E PoC demonstrated that age assurance could work using platforms and devices with which children and their parents are familiar. This is a significant achievement, nonetheless further age checking proof of concept work with a larger group is needed to understand how it would work at scale. VoCO 2 has provided the groundwork for expanding future testing to assist in making age assurance a reality.



Eco-system leverage points

[36] UAT trials involve actual users to test the software and ensure it works in real-world scenarios.

The E2E PoC looked to match the information provided by the child and digital parent against the data sources held by the age check provider. This would verify the parent-child relationship and the child's age alongside a service that can manage whether or not a parent has given consent for their child's data to be processed. This solution was also designed to empower the digital-parent to grant, deny and withdraw consent for the processing of their child's data. This solution creates an attribute token for verification of responsibility for a child, the age of the child, and verified parental consent. It also complies with applicable regulatory requirements, including the General Data Protection Regulation (GDPR).[37]

The Phase 2 proof of concept looked at two scenarios:

1. The solution is easily accessible to broadband customers and the trigger to get a digital parent to go through the process is initiated when a child wants to access, for example, an app. Here, the digital parent and child use their own devices and do not require significant education or support to complete the user journey. For this trial the age check provider partnered with a global Internet Service Provider (ISP) and a third-party app provider.[38]

Result: The outputs of this trial demonstrated that an age assurance request initiated by the child on an individual app could be completed by the parent who is a customer of the partnering ISP. This was enabled through the ISP's portal, which was integrated with the age check provider, and would respond to a request initiated by their child via a third-party app. Both parents and children's feedback were positive, thereby proving not only that it is possible to run a VoCO process seamlessly but that broadband customers can not only complete but continuously manage from within the ISP's portal.

2. The assessment of the child's age occurs during a home router set-up. This technical trial demonstrated that a parent-initiated user journey where a parent, setting up a home router can identify which devices on the network belong to children and adults, for example, a child's mobile device. Following this the digital parent can respond to a request from their child to access the app. For this trial the age assurance provider partnered with a cybersecurity company focusing on parental controls, device management, privacy and threat analytics.

Result: The trials ran successfully and there was positive feedback from both parents and, thereby proving that it is possible to run an age assurance process seamlessly while configuring a home router. As someone, usually a parent is required to set this process up, education is key to the continued success of this approach. It is important that the person setting it up understands the importance of what they are doing and when it would need to be refreshed, for example if the child was to get a new phone.

The trials provided a credible demonstration of the technology in use by 'real people,'. The trials were run in two schools and parents and children brought their own devices. In the future, with technical developments and innovation in the space, there may be other ways to address the VoCO challenge, but for now these VoCO trials demonstrate a technically viable, user friendly, privacy-preserving approach.[39]

Work was also undertaken by the VoCO team to research a number of other companies demonstrating a range of ways that age assurance could be achieved. Through the ACE consortium, we issued a survey on age assurance solutions and interviewed each company. This research is not being made publicly available for commercial reasons.

[37] This statement is based on self-assessments completed by the companies involved as well as a review by ACE under the framework agreement.
[38] An ISP is a company or organisation that provides internet access to individuals, typically through a computer or mobile device.
[39] Please refer to page 48, reference #9.

5. Imagining Ideal VoCO Futures

What would the internet of the future be like if age assurance was widely implemented and is effective, and the VoCO Manifesto for Change [pg 10] has been realised? This was the question posed at the final VoCO Phase 2 workshop. Attendees came together to co-create a series of VoCO futures and imagine what children's online experiences would be like if the VoCO Manifesto had been realised.

Our vision is that by actively recognising which of their users are children platforms create a positive sense of safety and opportunity online. Age assurance should not be a tool to create a 'walled garden' effect where children are isolated or confined into a reduced version of the internet. Key to this is a relationship of trust between Platforms, Digital Parents and Children.

The purpose was to create a 'creative tension' between where we are now and a future which delivers a safer internet for children. We hope that these help to encourage dialogue about children's internet safety, to stimulate creative thinking and to prompt stakeholders to action. We focused on the three, fundamental, online experiences for children. These experiences are platform agnostic and are likely to remain common experiences as technology continues to evolve.

- Chatting and socialising
- Gaming
- Creating and consuming content

We have set these VoCO futures 10 years in the future (2030) to help encourage stakeholders to think about the possibilities of age assurance and its benefits, without being constrained by current considerations. We applied the VoCO Manifesto to ensure that the futures are desirable and feasible for children, parents and platforms. The vision and principles set in the VoCO Manifesto provide the means to critique VoCO solutions objectively. The Task Force applied the Manifesto to challenge and refine three potential VoCO futures.

5.1 'On message' a VoCO Future

In 2030 children love to chat online. Messaging features are offered by most platforms, enabling conversations that involve text, emoji, images, sound, video and haptics to take place between individuals (peer to peer) and between individuals and groups. Wearable technology and improved communication infrastructure mean that children are able to communicate from any setting, 24/7, simply and effectively. Children have an expectation of privacy when they use messaging services and they also want to feel safe. They may not always be aware, however, that providers by law have a duty of care to protect all users from online harm.

ISSUE

The nature of private messaging services often prevents the detection of potentially harmful (and illegal) activities.

QUESTION

"How can platforms providing messaging services offer strong privacy and perform their duty of care to protect child users, whilst supporting the rights of the child (and other users)?"

In a VoCO future, the platform knows which of its users are children and safeguards them during private conversations, stepping in when necessary. By default, every conversation which involves one or more child users is subject to safeguarding measures. A combination of powerful analytics and AI automate the safeguarding function. Participants in online conversations are able to opt out; however, younger children require permission from their digital parents to do so and older children are provided with help and support to consider and manage their risk of switching these settings to a lower level of protection. The platform proactively enables children to make good choices, including their consent to apply age assurance methods. It is straightforward for children to exercise choice in relation to specific conversations, individuals and groups. This is recognised by the industry, who certify that the platform meets strong child safeguarding standards, enabling it to display a 'Trust Mark' on its products and services.

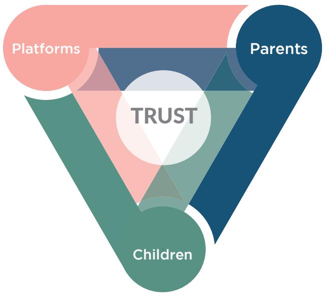
The knowledge that there is likely to be a safeguarding element to conversations encourages self-regulation within the online community (netiquette). Moreover, simple nudges from the platform are often enough to modify risky behaviour, and this proves to be a powerful disincentive for bad actors targeting children.

In 2030 the online messaging world is VoCO enabled. Here's what that means for safeguarding...

Widespread use of AI and analytics to safeguard children generates deep understanding, which enables risk of harm to be allocated effectively to those parts of the ecosystem which are best placed to manage it.

Digital parents have peace of mind that the platforms are protecting their child's privacy rights are being respected; this is supported by 'Trust Marks'

Effective regulation ensures the platform is held to the same standard as its competitors. The risk presented by the company takes precedent over its size.



Parents are empowered to help younger children make good choices on their online safety. Including about the platform's use of age assurance data sources, privacy settings and whether to opt out from safeguarding measures.

The platform recognises which of its users are children and takes active steps to safeguard them from harm.

It is considered normal, indeed appropriate, to have a safeguarding element in individual and group chats with peers and mixed age users.

Children feel safe, yet have considerable leeway to take risks and learn from experience online; this (coupled with effective help and support) increases their resilience.

Children recognise that they are neither missing out or nor having a worse experience through retaining their opt in. Unwanted onward sharing and bullying become an exception.

5.2 'Play it Safe' a VoCO Future

In 2030 children love to play games online. E-sports are part of the national curriculum and the most popular massive multiplayer online games provide completely immersive, virtual and augmented reality experiences. Despite parental and societal concerns about compulsive design, children engaging in online gaming are entertained and benefit socially from a strong community of interest. They are not, however, legally entitled to earn money as gaming professionals.

Gaming platforms know an extraordinary amount about individual gamers' physiology and psychology, enabling them to customise games in real time to cater to an individual's personality and mood. Advanced analytics match gamers to maximise the fun and to maximise commercial gain within global e-sports leagues.

ISSUE
Children are attracted to online games which contain mature themes and older players; bad actors are attracted to online spaces where children congregate.

QUESTION
"How can platforms provide an online experience for children that is safer and more fun?"

In a VoCO future, the platform performs an assessment of the user's age and corresponding safeguarding requirements, which helps protect children when they are gaming and interacting with their peers online. The platform uses features of the end-point devices used within the game to validate the player's declared age and combines this with their gaming preferences to perform a 'child safety assessment'. A tokenised and encrypted output from this process can then add the player to an 'allow list' which would effectively mark the player as 'desirable' and subtly modifies their gaming experience.

During game play the platform continues to increase its age confidence in the age of the user, employing a wide range of age checking sources, including industry trust frameworks. Age assessment is combined with analysis of in-play preferences to continuously refine the child's safety assessment and online experience, including the players with which the child is matched. Severe mood changes and other indicators of potential harm (such as excessive in game purchasing) are detected and trigger a safeguarding response to the child and (where appropriate) their verified digital parents.

In 2030 the online gaming world is VoCO enabled. Here's what it feels like within the gaming community...

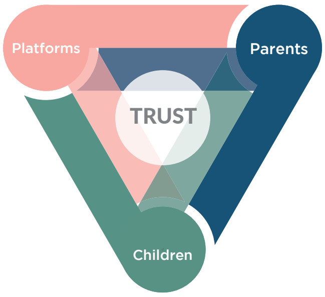
The gaming industry benefits from an enhanced gaming experience and brand: the 'mavericks' are widely recognised as unsafe spaces, losing players and mainstream marketing spend.

Parents don't need to keep up with fast changing gaming fads and trends. They know that younger children will not be able to access the platform (for long) if they lie about their age and that the platform safeguards older children whilst they are online.

Age confidence plus child safety assessments are an effective way to identify risks and ensure they are managed through in game experience.

Influencers in the gaming community support and promote the VoCO enhanced gaming experience.

It is in the platform's interest to know which of its users are children and provide an appealing experience which takes into account their individual preferences and vulnerabilities.



Strong industry and regulatory standards protect data privacy and security. Digital parents and their children are comfortable with end-point device enabled age assurance, because they trust the platform.

Parents understand that older children will not want younger siblings to use their profiles (with or without their permission), because this will adversely affect their gaming experience.

Children know they are being protected from 'the bad stuff online' but don't feel they are missing out or their experience is diminished. This, coupled with effective help and support increases their resilience.

There is no incentive to lie about your age in online gaming - the reverse applies.

Children of secondary school age and above are happy to buy-in to this future; modifications to their gaming and related community experience are subtle and build confidence, without restricting exceptional individuals' growth as gamers.

5.3 Content with Content

In 2030 children love to consume content online. All children grow up surrounded by online content. Despite significant technological advances in the way that content is created and shared, there remain key development points for the digital child;

1. When they no longer consume content through devices 'owned' by their digital parents;
2. When they first attend secondary school; and,
3. When things go wrong for them online.

ISSUE

Children can be unintentionally harmed online by exposure to legal content that is intended for adults, and bad actors seek to cause harm through the creation and sharing of content; this is exacerbated by sudden 'cliff edges' in a child's digital development.

QUESTION

"How can content platforms support each child's journey from digital infant to mature digital adult in a way that safeguards them, whilst enabling them to develop confidence and resilience online?"

In a VoCO world, the general content platform co-operates with other suppliers to ensure it knows which of its users are children.

A comprehensive industry Trust Framework makes it easy for children and their digital parents to sign up for new content services. The concept of separate accounts for different content platforms is obsolete. Encrypted, anonymised tokens provide dynamic levels of assurance about a child's age in accordance with the level of risk inherent in the platform and way it is being used. In addition, users below the age of 18 are encouraged to identify as children if they access content through end-point devices owned by others. Self-declaration is supplemented by a range of age assurance methods including biometrics and behavioural analysis. Users can opt out from automatic age checking; however, the reduction in age confidence affects their online experience. As a further safeguard, the platform's estimated age band for the content consumer is flagged, prominently, through the user interface.

Age assurance makes it possible for content providers to modify the experience for children based on their age and verified digital parents' preferences, rather than reinforce boundaries that produce a step change at age 13 and 18. Children are gradually exposed to more mature content and related online behaviour. They are also better protected from immature decision making about creating and sharing content. Content providers recognise that children are constantly developing and maturing in a range of settings, and that they may change their opinions over time. They supply regular support and advice as part of their service, empowering children to make informed choices about age checking and the effect that this has on their online experience and digital footprint.

The online community applies a common set of rules to classify content and channels thematically, which enables the platform experience to be tailored for individuals and groups according to their age (band) and preferences.

Greater confidence about the age of their users also means that platforms are more effective at targeting the identification and removal of content which is harmful to children, including self-generated sexual imagery. Where it suspects there may be a risk of harm, the platform provides age appropriate advice and support to the child and verified digital parent.

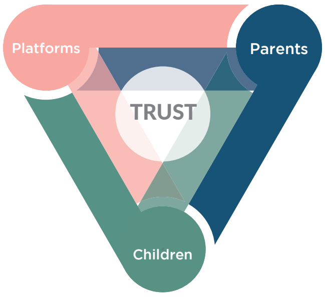
In 2030 the online content world is VoCO enabled. Here's what it feels like as children grow up...

Age confidence enables the platform to target advertising and include personal information in the user experience (where legal to do so); consumption of young children's content by older children and adults can be monetised.

A simple visual indicator on the device interface provides parents with peace of mind that the content provider knows the user's age range and has modified the experience accordingly.

A clear platform policy for different age ranges provides a powerful way to identify risks and ensure they are managed through the child's online experience.

Accounts don't matter for consuming content*; there is no multiple accounts issue. (*They do matter if you're a content creator)



Setting age bands for consumption of content is normalised; parental preferences apply to younger age bands.

Children are no longer suddenly exposed to adult behaviour because they pretend to be age 13+ when they were younger

Children are gradually exposed to mature content and related online behaviour, helping them to build up confidence, understand risk and develop resilience at their own pace.

Children know they are being protected from the 'bad stuff online' but don't feel they are missing out or their experience is diminished.

Older children are no longer concerned about their digital footprint and the risk they made poor choices about creating and sharing content when they were less mature

There is no incentive for children to lie about their age when they obtain their own end point devices, because the experience is the same on all devices.

6. Conclusions and Takeaways

The VoCO project has attempted to imagine a better internet for children. The project has emphasised the value of bringing together a broad range of stakeholders to learn from each other and to advance attitudes around the role of a user's age as a form of online identity.

VoCO Phase 2 has continued to explore what is needed for platforms to recognise their child users and adapt the spaces they use to make them safer. We have engaged children, parents and platforms to help us understand their differing perspectives, using their views to develop a Manifesto for Change to guide us on our journey towards a safer online experience for children.

The concept of age assurance developed in VoCO Phase 2 is purposefully broad. It is designed to drive innovation and provide sufficient flexibility and transparency to drive commercial and, in the future, regulatory incentives for platforms to establish the age-band of their users.

During Phase 2 we explored the ways that age assurance can be achieved. We also took this further by running a technical trial that demonstrated how different services in the 'internet stack' can scale age assurance, and share trusted age-band and consent tokens in a frictionless privacy-preserving way. The results of this proof-of-concept shows that it is possible to scale age assurance by decentralising the steps required to achieve it.

Over the last 12 months, through the two phases of this project, we have explored the concepts, frameworks and practical implementation of platforms knowing which of their users are children. Whether it is supporting new technologies, uplifting standards or creating new norms of practice, it is important that a collaborative approach is taken.

To progress this work we have highlighted four areas that are key to delivering an internet that actively recognises children:

1. A regulatory strategy for age assurance

The successful realisation of the VoCO Manifesto requires a broader regulatory context. There is growing momentum to take regulatory action to tackle online harms. In the last 12 months we have seen the laying of the ICO's Age Appropriate Design Code in Parliament and the UK government's initial response to the Online Harms White Paper. In March 2020, the Five Country Ministerial published the Voluntary Principles to Counter Online Child Sexual Abuse, which has been publicly endorsed by six major technology companies and government will publish later this year a voluntary code for industry on countering online child sexual exploitation and abuse. Common throughout all of these pieces of work is the importance of platforms understanding which of their users are children, and the role of age assurance in achieving this.

It is important that regulation does not create an adversarial environment where children are incentivised to find new ways to lie about their age, where digital parents are unduly burdened with requests to age assure, or where responsible companies are put at a commercial disadvantage for keeping children safe. Key to this is risk-based and proportionate regulation that engages fully with the technology landscape and stays abreast of developments in technology. **We recommend:**

a. **Undertaking research on the risks posed to children by online services, to help inform the proportionate and risk-based use of age assurance.** This research should engage with industry and subject experts.

b. **Action is taken to secure regulatory alignment between relevant current and emerging regulatory frameworks.** Government should explore forming a 'task force' of government and relevant regulators.

2. Encouraging industry's adoption of age assurance

During VoCO industry engagements it was stressed that companies are committed to protecting children online. However, our research found that many do not have access to the details of the risk posed to children on their platforms and that there is a lack of agreed best practice on how to mitigate these risks. Platforms also expressed concerns over how mitigation action, including age assurance, would be reflected in their liability and the commercial viability of implementing such actions. **We recommend:**

a. **Developing industry benchmarks, facilitated through**

research on the risks posed to children by online services. This research should engage with industry, regulators and subject experts.

b. **Developing best practice examples,** in collaboration with regulators and industry.

3. Stimulating innovation in age assurance

During Phase 2 we explored what was needed to help industry innovate and strengthen its age assurance offer. We looked at the various methods, data sources, standards and frameworks applicable to stimulating age assurance innovation into the future.

Part of this work has been developing an agreed definition for age assurance and defining the processes that take place to perform it. This work looked at the relationship between the risk presented by a platform and the corresponding level of age confidence needed when performing age assurance. It has explored the benefits of pursuing Age-Checking to minimise the processing of personal data and explored how to scale age assurance through age-check exchanges (please see Section 3.7).

The work also looked at the many frameworks and standards that relate to establishing age online. As no single existing standard or framework can enable the VoCO Manifesto alone we looked at what a template standard, or set of standards might contain. **We recommend:**

a. **Action is taken to promote the age assurance market** among industry and users.

b. **Supporting the development of industry standards** to ensure consistency and trust in age assurance solutions.

c. **Exploring accessibility to testing data,** to improve accuracy in age assurance methods. This is particularly important for methods that rely on training an algorithm, such as age estimation based on biometric data.

d. **Taking action within the engineering and design community** to ensure that age assurance is built into design codes of practice.

4. Growing public confidence in age assurance

During VoCO engagements with digital parents and carers it was clear that the online safety of their children was a priority. It was strongly felt that children should be safeguarded online, their privacy protected, and that they should be able to benefit from the freedom and opportunities that the internet offers. However, this balance was felt at times to be in tension. Foster parents and carers of vulnerable children felt this particularly acutely. It is clear that protecting these, often already vulnerable children, needs to be considered more closely. In general we found digital parents expressed frustration with the lack of simple safeguarding measures on platforms. **We recommend:**

a. **Undertaking research into how age assurance may disproportionately impact on some children,** and explore how these insights can be reflected in the development and implementation of age assurance.

b. **Supporting digital parents to gain a better understanding of the safeguards that age assurance offers,** and the compliance action taken by providers and platforms.

7. Appendices

7.1 Phase 1 Recommendations

Outlined in the table below are the detailed Phase 1 recommendations and the activities that were performed in Phase 2 in support of those recommendations.

VoCO Phase 1 Recommendation	*Relevant Phase 2 Activities*
1. Validate proposition of a trust framework and attribute exchange by recreating the full, integrated end-to-end technology chain and incorporating relevant attribute providers, data sources and platform integrations.	Perform end-to-end proof on concept utilising Trust Elevate platform.
2. Engage with Infrastructure Providers including Application and Operating System Providers and Telecommunications Operators directly to better understand feasibility and effectiveness of these potential early interventions, and their role in VoCO.	As part of the end-to-end proof of concept, worked directly with British Telecom as the broadband provider and BlackDice via the home router to test technical feasibility. Also included infrastructure partners into CIPL industry round table discussions.
3. Review Standards and Data Sources to identify all relevant standards to online child protection and potential identity attribute providers, including existing AV providers and holders of authoritative datasets.	Deployed two separate workstreams to 1) review the universe of existing standards and provide recommendations for future consideration, and 2) assess the relevant universe of data sources and the implications of utilising each of those data sources for Age Assurance.
4. Review Age Confidence Scoring in the context of VoCO, accompanied by a feature-based risk assessment of mainstream platforms to understand how confidence can be meaningfully handled in the context of a particular platform's risk profile.	Began to define levels of assurance and associated requirements for broad risk levels as part of workstream activities.
5. Community of Interest Portal where a wider group of stakeholders can share understanding of similar initiatives and standards to ensure alignment and avoid siloed thinking.	Convened three workshops with a range of participants to provide input and feedback to shape VoCO moving forwards.

6. Engage with Children and Young People, including those living in a range of different circumstances, to de-risk the concept of VoCO and identify barriers and incentives to adoption.	Held workshops and interviews with children across a range of ages and socioeconomic situations to test and inform the VoCO manifesto principles.
7. Engage with Digital Parents, that is, all biological, legal, corporate parents, those in loco parentis and so on, to de-risk the concept of VoCO and identify barriers and incentives to adoption.	Held workshops and interviews with digital parents to test and inform the VoCO manifesto principles.
8. Engage with Industry to de-risk the concept of VoCO and identify barriers and incentives to adoption.	Held industry round tables to share the current thinking regarding VoCO and solicit input on what would be required from Industry's perspective to make VoCO feasible.
9. Engage with adjacent sectors, e.g., fintech, to better understand what tools, governance, legal frameworks, testing and test data they required to make progress in that sector.	Adjacent sectors were invited to participate in each to the three workshops with their input shaping Phase 2 outputs.
10. Utilise an agile methodology to conduct the above recommendations	Utilised an agile methodology as outlined in 7.2 below.

7.2 Methodology and Approach for VoCO Phase 2

Multi-phase Process

Phase 2 was completed over 18 weeks between October 2019 and March 2020 and as direct follow-on to VoCO Phase 1. The Home Office ACE team in partnership with the GCHQ Counter Child Sexual Abuse (CCSA) Industry Team executed the accelerated process to advance the VoCO hypothesis and begin to understand how VoCO might be achieved.

Multi-stakeholder Process

The identification and determination of insights within this report required a holistic approach in order to ensure that any recommendations considered the perspectives of children, digital parents and platforms. The project convened a group of subject matter experts from a range of disciplines to comprise a Task Force. This Task Force met on a monthly basis over a 12-week period, utilising the services of a professional facilitation company and adopting a participatory approach to problem-solving. This involved fostering creativity and lateral thinking within a space where differing (and at times competing) expert positions could be held equal to one another.

The multi-disciplinary Task Force that led this work comprised the following skill sets:

- Technology experts with backgrounds in software development, cybersecurity, and information management.
- Legal experts, with backgrounds in privacy, security and human rights.
- Policy makers from government, regulators, safeguarding and the education sector.
- Children's rights and third-sector organisations.
- Practitioners, including social workers and child internet safety educators.

- Representatives from the internet industry, who were engaged as part of a series of roundtables with attendees from social media, online gaming, app stores, Internet Service Providers and mobile operators. This engagement strand included follow up 1-1 interviews.

This approach explored multi-faceted elements of children's online activities, real-world circumstances and the roles and responsibilities of those stakeholders who are responsible, in whole or in part, for children's online safety - this included tech companies, government, regulators, parents, teachers, and social workers. The discussions included consideration of real-world ramifications, in both political and family spheres. Discussion considered the erosion of public confidence in online platforms, and parental concerns about children's wellbeing online. These factors have in part driven the current political response, for example the government's Online Harms White Paper, which identifies the duty of care online services and platforms have towards children and young people.

7.3 Understanding the Situation for Children and their Digital Parents Today

Critical to the VoCO project is understanding the problems that children and their digital parents face when it comes to online safety. This Appendix combines a number of insights drawn from our research and expert engagements on today's digital landscape, which have informed the VoCO project as a whole.

Children value their online lives, and in many cases consider it central to their overall sense of self. But inextricably linked to their online experience is exposure to harms.

Increasingly, children are living a significant proportion of their lives online. The experience can be positive for children by providing the opportunity for social networking, connecting with their peers, and accessing a wide array of educational resources, information and entertainment. The social impact of their online lives can be particularly meaningful. Research by Ofcom found that 9 out of 10 social media users aged 12-15 stated that using social media has made them feel happy or helped them feel closer to their friends.[40] However, as outlined in the government's Online Harms White Paper, illegal and unacceptable content and activity is widespread online and users are frequently concerned about what they have seen or experienced. The impact of this harmful content and activity can be particularly damaging for children and young people. With the average teenager in the UK spending 18 hours a week on their phones, and much of that on social media, there are growing concerns about the potential impact on mental health and wellbeing and what this might mean for future generations.[41]

Online environment today and its impact on children

Children view potential harms as endemic to their online experience, but this is outweighed by children's perceived need to engage online.

Given children's developmental vulnerabilities, such as proneness to peer pressure or more limited ability to consider or weigh up long-term consequences, there are certain online harms to which children are particularly susceptible.[42] The extent to which a child is vulnerable can also vary significantly depending on the circumstances of that child. Children who are vulnerable offline are frequently the most vulnerable online.[43] This was highlighted during VoCO engagements with digital parents. A foster carer highlighted how children in his care had experienced significant difficulties that were exacerbated by the platform's functionalities, for example private messaging or live streaming functions.

> **There's been instances where our girls in our care have put themselves in very risky situations using [social media platform], sending indecent pictures, which has become quite normal for young people.**
>
> **– Foster Carer [44]**

[40] HM Government, 'Online Harms White Paper,' 2019
[41] BBC, 'Social media apps are deliberately addictive to users,' 2018
[42] Internet Matters, 'Vulnerable Children in a Digital World', 2019
[43] Ibid
[44] Please refer to page 47, reference #1

During VoCO engagements with children it became apparent that for them online harms are expected and are endemic to using the internet. Over the course of the Child's Voice workshops, children from primary to secondary school age and from a mix of schooling types, expressed that they themselves were exposed to these harms or personally knew of someone who was. They were comfortable talking to experts about the fact that they had commonly been approached by adults they did not know, were familiar with bullying and with viewing upsetting content, and were very 'matter of fact' about their negative online experiences.[45] Even in cases where the children had experienced real difficulty and distress online this did not translate to them as a reason to avoid the online environment – they saw the negatives as simply an unavoidable part of their lives. Child Sexual Exploitation and Abuse (CSEA) is frequently highlighted in reports about online harms affecting children due to its seriousness, scale, and the extent of its negative impact. However, there are a broad spectrum of online harms and wellbeing issues impacting children on a day to day level.

Compulsive Design

> **I think sometimes we're not even aware we're so focused on it. Say 'likes' for example, or posts, it's easy to say 'I'm not bothered by it, how many likes I've got', but when you're actually on it you forget. If it doesn't get likes you delete it**
>
> **– 15 year old girl[46]**

Many social media apps have been designed to encourage frequent use. For example, features such as infinite scrolling, which allows the user to continuously scroll or swipe through content without friction. The sense of validation or feeling of acceptance provided by social media engagements can impact on wellbeing, particularly for children. BBC Panorama found that 'Likes' can provide a sense of validation.[47] The 'Life in Likes' 2018 report from the Children's Commissioner also show the lengths that some children go to for likes, for example children aged 11-12 often use strategies to encourage likes such as warning their friends before sharing a photo or video on social media so they can like it.[48]

Cyberbullying

> **A couple months ago I was being bullied by a group of boys. Then somebody without my permission shared it (a video) on [social media platform] and [another social media platform]. Yeah, I was so distraught and basically crying randomly in class. Everyone was making comments about it. I didn't see the video myself, but other people saw it on their phone so I don't really know who sent them**
>
> **– 14 year old boy [49]**

Despite the many positive experiences that children have when they are interacting with friends online, it is apparent that there is commonly a problem with bullying in the online environment. Cyberbullying is a common experience, with children acknowledging that it is easier to perpetrate because it is not face-to-face. Internet Matters report that one in five 13-18 year olds claim to have experienced cyberbullying.[50]

> **I would rather be bullied face-on in real life or even hit in real life**
>
> **– 15 year old boy [51]**

> **Cyberbullying is worse than bullying in real life because you don't know who is doing it**
>
> **– 14 year old boy [52]**

The Online Harms White Paper made reference to the fact that cyberbullying can have psychological and emotional impact, with the negative effects often more intense than in the off-line world.[53]

Self Generated Indecent Imagery (SGII)

> **She was probably 12 at the time. I would say there was more sending of nudes when I was 12 or 13 than there is now and I'm 16**
>
> **– 16 year old boy [54]**

The sharing of underage sexual imagery, or self generated

[45] Please refer to page 47, reference #1.
[46] Ibid
[47] BBC, 'Social media apps are deliberately addictive to users,' 2018
[48] Children's Commissioner, 'Life in Likes', 2018
[49] Please refer to page 47, reference #1.
[50] Internet Matters, '10 things you need to know about cyberbullying', 2020
[51] Please refer to page 47, reference #1.
[52] Ibid
[53] HM Government, 'Online Harms White Paper,' 2019
[54] Please refer to page 47, reference #1.

indecent images, can lead to regret and a sense of exposure, as well as bullying and harassment. The scale of the problem is hard to assess, as many children do not report incidents. However reporting from the Internet Watch Foundation (IWF) earlier this year suggests it is most prevalent for 11 to 13-year old children. In 2019 the IWF took action on over 37,000 reports of self generated images of under 18s.[55]

During the VoCO workshops with children, children understood that sending an inappropriate personal picture may not be in their best interest. However they shared that the pressure they feel under in their relationships or friendship groups overrides any doubts or concerns they may have. This was further highlighted in conversations where children stated that they did it to "show off, just to be like I done this" and the impact of peer pressure, "Yeah, under pressure to send pics. Mates all do it, so then they do it".[56]

Data privacy

Although not unique to children, young people are at risk of having their data used in ways that are not privacy preserving or are not clearly explained to them. Children are often unaware of how their online activity - e.g. browsing history, social media networks, and postings - drives much of the content that they see. Research by Doteveryone suggests that 62% of people do not realise that their social networks can tailor the news they see, while only 3 in 10 adult online users questioned by Ofcom were aware of the ways in which companies can collect data about them online.[57]

Instantaneous engagements

> **The main thing in our school is taking photos of yourself... most of the time if you have a girlfriend. You send it to them and they can just screenshot it like that. If anyone says anything to them, they could say, well I got this by here and send it around**
>
> **– 14 year old boy [58]**

Aggravating these online harms is the fact that thinking time is eliminated. Online interactions are often immediate and instantaneous. Children do not always have the time to rationalise and choose what information they share and with whom they share it. The opportunity to change their mind during a period of imposed reflection is often no longer there.

> **I know people have done stuff on [social media platform] they regret. I've said stuff in anger... it's not deadly serious. Our age the thing we regret is sending stuff**
>
> **– 16 year old boy [59]**

The online environment is rapidly evolving. New platforms and technologies can rapidly scale, acquiring new users - including child users - at an unprecedented speed. The table below illustrates how fast the technology landscape has changed and been adopted by users. The pace of adoption is accelerating and is likely to continue to do so going forward.

Technology	***Average time taken to hit 50 million users***
Radio	38 years
TV	13 years
Internet	4 years
YouTube	10 Months
Pokemon GO	19 Days

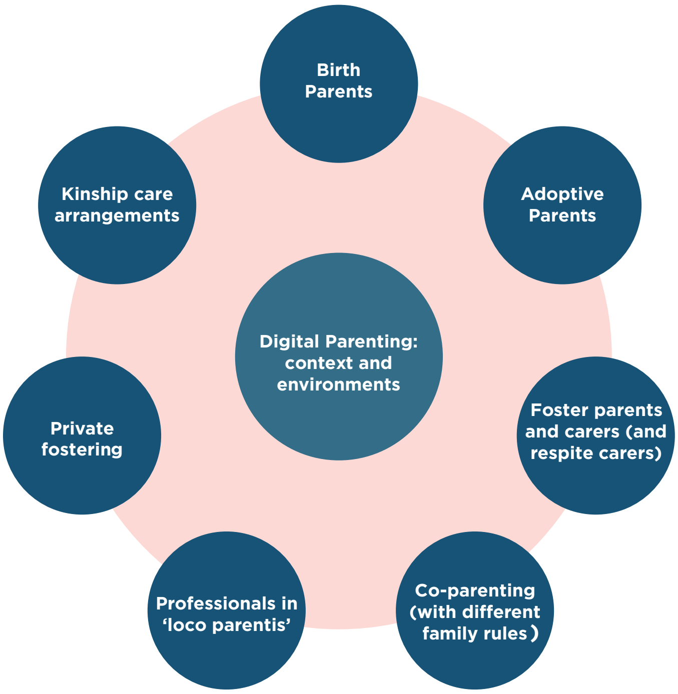
How long it takes technology to hit 50 million users [60]

The online environment today and its impact on Digital Parents

Digital parents are overwhelmed and feel that current solutions to protect their children are inadequate. They feel trapped - having to choose between banning access and isolating their children from peers, or allowing access and risking harm.

In the context of the online environment, the parental responsibilities can extend to a range of individuals in a child's life, not just the biological parent. For this reason, when discussing the online environment, VoCO uses the term 'digital parent,' to include the more comprehensive scope of people with responsibility in safeguarding children.

[55] IWF, 'The Dark Side of a Selfie', 2020
[56] Please refer to page 47, reference #1
[57] Ofcom, ICO, 'Internet users' concerns about and experience of potential online harms', 2019
[58] Please refer to page 47, reference #1
[59] Ibid
[60] Interactive Schools, 'How long does it take tech to reach this milestone?', 2018


Birth Parents
Adoptive Parents
Kinship care arrangements
Digital Parenting: context and environments
Private fostering
Foster parents and carers (and respite carers)
Professionals in 'loco parentis'
Co-parenting (with different family rules)

Digital parenting considers both context and environment. As children move through the analogue world, digital parents also evolve

A recent research study by Global Kids Online found that many digital parents feel as though their options are at two ends of the spectrum – either to allow their children access to online platforms and the potential exposure to harm, or engage in restrictive mediation. Parents reported restrictions such as setting rules that limit time spent online, location of use, as well as content and activities. These restrictions have the potential to isolate children from their peers. VoCO engagements with digital parents made similar findings.

> **She likes to use social media sites which are all obviously not meant for her age group. Again, she wants to fit in. Social media is very difficult to police... I feel there is an element of peer pressure to go on these sites. I don't want her to go behind my back, so I let her go on and monitor what she's doing**
>
> **– Parent to a 10 year old girl**[61]

A survey by Internet Matters found that in young children (6-10), digital parents want to allow children greater freedom in using devices. Digital parents want to provide children an opportunity to explore and build up resilience. However, they are concerned that children will unintentionally put themselves in harm's way by seeing inappropriate content or being contacted by people they do not know.[62] Our own research with parents and carers showed that parents had significant concerns about their children's current internet use and in particular sexual and violent content.[63]

> **My 8-year-old son likes to play [multiplayer game] which I worry is too violent. He wants to fit in as all his friends are playing it. ... my worries are that he's talking to strangers. It is very difficult to monitor what he's doing on there and who he is playing with as he jumps from game to game**
>
> **– Parent to an 8-year old boy** [64]

Many digital parents try to put in place safety settings or monitor their children's online activity. The VoCO engagements with younger children found that they themselves view their digital parents as key stakeholders in their online experience. For these reasons, many digital parents continue to directly monitor their children's internet usage. In a focus group of primary school age children, 17 of 18 pupils stated that their parents monitor their internet usage.

Many of the parents that were spoken to as part of the VoCO engagement spoke about using a mix of strategies, including talking to their children about what they were doing online, as well as using technical means. Approaches mentioned included 'safe search', reviewing their children's devices or apps, and time limits.[65] However, almost all the parents spoken to as part of VoCO found it challenging to keep up to date with what their children were doing and the majority of those engaged with wanted the technology industry to do more.

> **I have a duplicate app so I can monitor some things she is doing but it is impossible to monitor everything. For example, [a social media platform] had an age restriction and I allowed her to go on there, mainly so she didn't go behind my back and go on anyway. But I can't actually police it. I have no idea who is watching the videos and I can't see what my daughter is doing on there all the time. I also worry about what she is watching on there too**
>
> **- Parent to a 10 year old** [66]

A recent survey by Internet Matters found that at the pre-teen age (11-13) digital parents feel that children are starting to

[61] Please refer to page 47, reference #1.
[62] Internet Matters, '2018 Survey', 2018.
[63] Please refer to page 47, reference #1.
[64] Ibid
[65] Ibid
[66] Ibid

distance themselves and feel less aware of what their child is doing online, leaving them feeling concerned that their children will actively engage in dangerous behaviours.[67] In line with developmental norms it is generally the case that children continue to want more freedom and less scrutiny from parents as they move into their teenage years (14-16), and in many cases children become the comparative family experts in the online world. This was evidenced through the VoCO workshop discussions where many of the teenagers expressed a strong sense of confidence about their online lives and their ability to handle issues themselves. There often appears to be a tension here as parents try to strike the balance between establishing rules and boundaries, and building trust.[68] This tension was particularly evident in one of the engagement sessions with a group of 12-15 year-olds (most of whom were 14 or 15). The young people highlighted that they found it intrusive when their parents tried to monitor their access to the internet. They explained that when their parents asked to see their phones they would not find anything because they knew how to hide or delete apps before allowing their parents the opportunity to review them.[69]

> **It's strange that I wouldn't drop my 14-year-old off into a nightclub with around 500 random strangers and leave her by herself but I'm allowing her to go on these apps and sites where they could be just as vulnerable. We're not set up for that, we're not prepared for that. It's not what we expect, we expect them to be safe and they should be allowed to be safe.**
>
> **– Foster Carer** [70]

The tension created between parents and carers and their children in their efforts to keep them safe online was also evident in the parenting of particularly vulnerable children. The VoCO engagements with foster parents and carers showed how some of the foster carers struggled with some of these challenges – the difficulty of trying to monitor and keep children who are very vulnerable safe, whilst at the same time defending their rights to online freedom and access. One foster carer shared how his foster daughter had been groomed online and had met up with the stranger without them knowing. They had to involve the police. The same carer had also, in another situation, attended a strategy meeting to challenge the proposal that one of the children in his care should have a complete ban on social media. He felt this would result in undue distress and social exclusion for the child. A takeaway from our VoCO engagements was that foster parents and carers particularly struggle with the challenge of striking a balance between safety on the one hand and freedom and opportunities on the other.

Children's rights and the balance between privacy and safety

Balancing safety and privacy is an important element of the VoCO Manifesto. Offline, there are systems in place designed to promote children's rights, whilst also protecting them from harm. For example, in the UK, 'Keeping Children Safe in Education' articulates a child centred approach to safeguarding children in schools and colleges that always considers what is in the best interests of the child. The framework balances the safeguarding objectives against the rights and wishes of the child stating that systems should be in place for children to express their views and give feedback.[71]

At a global level, the United Nations Convention on the Rights of the Child (UNCRC) and 5Rights Foundation have articulated the specific rights all children should be afforded. The UNCRC states that every child has rights whatever their ethnicity, gender, religion, language, ability or any other status. The 54 articles cover all aspects of a child's life and set out the civil, political, economic, social and cultural rights that all children everywhere are entitled to.

However, translating these rights from the offline world to the online environment has been difficult. If pushed too far, efforts to protect children can infringe on their right to information and participation. A good example of this is internet filters. The Child Rights International Network have suggested that, without care, web filters could block a disproportionate number of sites to the point that a child's UNCRC Article 17 right to information and UNCRC Article 24 right to information about their health may be compromised. For example, filters may block sites about sexual health, being LGBTQ, or sites that lay out what to do if children have received unwanted contact online.[72] As drafted, the UNCRC does not specifically address the rights of children in a digital environment. However, the UN has typically asserted that the rights people have offline must also be protected online. A 'General Comment' on children's rights in relation to the digital environment is in the process of being developed by the UNCRC supported by the 5Rights Foundation.

[67] Internet Matters, '2018 Survey', 2018.
[68] Ofcom, ICO, 'Internet users' concerns about and experience of potential online harms', 2019.
[69] Please refer to page 47, reference #.
[70] Ibid
[71] HM Government, 'Keeping children safe in education', 2019
[72] United Nations, 'The United Nations convention on the rights of the child', 1989

Aligned with these objectives is the Information Commissioner's Age Appropriate Design Code, which seeks to improve the safety and rights of children through enhanced provisions for the protection of children's data. These provisions will ensure that the best interests of the child are a primary consideration in the design and development of online services, and that children's data will not be used in ways that are detrimental to their wellbeing.

The intention of VoCO is not to create a 'walled garden' effect where children are isolated or confined into a reduced version of the internet. Nor should it create an environment of distrust. The objective of the VoCO Manifesto is to create a positive sense of safety and opportunity online, similar to a good school where students are given freedom to be themselves and to explore life, but within a safe environment.

Why don't all platforms already recognise their users?

Regulation of child-directed websites and online services has improved the protection of children, but a substantial gap still exists for general audience sites that appeal to children.

> **most people lie about their age but they do that because there is a rule. If they didn't make a rule about how old you need to be, people wouldn't have to lie**
>
> – 15 year old girl [73]

In effect since 2000, the Children's Online Privacy Protection Act has been a significant piece of child safety legislation; its goal being that for children 13 or under their parents are placed in control over what data is collected about them. Under COPPA, online services directed towards children, or services that have knowledge of users under age 13, are required to obtain parental consent before collecting personal information. However, there are four exceptions which allow a one-time use multiple online contact with simply a notice to a parent:

1. Responding to a one-time request from a child, provided that the child's personal information is deleted after the response is made;
2. Collecting personal information in order to send the child periodic communications such as newsletters, provided that the parent is given the opportunity to opt out;
3. Where necessary to protect the safety of a child participating in the service; or
4. Where necessary to protect the security/integrity of the service, respond to a judicial request or other public investigation.[74]

COPPA effectively prohibits behavioural advertising, retargeting or profiling on most websites and apps that are targeted towards children. For websites and online services that target children, all users must be treated as if they are children with COPPA protections applied to all.[75] As a result of COPPA, for the majority of children's websites, key privacy protections have been implemented. Where companies have failed to provide adequate protections, the Federal Trade Commission has utilised COPPA to level fines against companies for collecting children's personal information without parental consent.

> **I lied on [a social media platform] about my age and people were wishing me happy 80th birthday**
>
> - 15 year old girl [76]

Under COPPA, websites are not required to investigate the ages of users. However, if general audience websites have actual knowledge that a portion of their users is under the age of 13, they are subject to COPPA rules and enforcement. Although developed with the intent to protect children's personal information from commercial exploitation, an unintended consequence is that COPPA acts as a disincentive for general audience platforms to recognise which of their users are children. To evade exposure to COPPA, online platforms have reacted by avoiding collection of age or date of birth or explicitly prohibiting users under age 13 from using the service in terms and conditions.[77] The experience of being banned was highlighted in VoCO engagement with primary school aged children. One 10 year-old girl stated that a widely used social media platform is always taking her account down, this was due to evidence that her account was in violation of community guidelines as she was not 13.[78]

Many platforms have responded to COPPA by implementing age-screening mechanisms, which in practice rely exclusively on the users' self-assertion of their age. A common consequence is that underage users lie about their age in order to bypass restrictions or parental consent requirements. The resulting dynamic for general audience platforms is an incongruence

[73] Please refer to page 47, reference #1
[74] Macenaite, M, 'Consent for processing children's personal data in the EU: following in US footsteps?', 2017
[75] Ibid
[76] Please refer to page 47, reference #1
[77] Macenaite, M, 'Consent for processing children's personal data in the EU: following in US footsteps?', 2017
[78] Please refer to page 47, reference #1

between intended audience and actual audience. Platforms do not recognise their actual user base and children continue to use platforms designed for adults.

7.4 Developing the VoCO Manifesto and Principles

The principles were developed through engagements with platforms, digital parents and children, as well as research activity and the Phase 2 workshops. They are not intended to be considered as final. This section looks at the evidence supporting each of these principles.

Platforms

For platforms, the VoCO principles are focused on having consistent frameworks to understand risk and liability while minimising the commercial impact.

Platforms Principle #1

As a platform, if I'm going to recognise and protect my child users... *I want a clear understanding of the risks they face on my platform*, and the practical measures required of me to protect them.

Platforms shared that they needed a comprehensive and dynamic risk assessment to help guide their application of age assurance methods, including the level of age confidence needed. To have business confidence companies shared that they needed assurances that they were following best practice, for example if the level of risk is minimal are we willing to accept a lower level of age confidence? Platforms present different levels of risk to a child , some will likely need 95%+ age confidence, while for other platforms it may be acceptable to carry a lower level of confidence. Although initial reactions, industry reiterated the need for a risk-based approach to determining the application of age assurance as well as the need to establish a common language and an understanding of roles and capabilities.[79]

Platforms shared that they do not always know all the details of the risks presented to children online, for example online CSEA or cyberbullying. They felt that a collaborative effort between industry, subject experts and government could enable the creation of a comprehensive mapping of risk that would help inform their service design and safety processes. VoCO found that this may benefit industry, in particular smaller organisations, as VoCO industry engagements showed that whilst companies are committed to protecting children from online harms, they do not normally share insights or good practices in relation to age assurance.

> **Our services are for adults aged 18 and over, and we will continue to implement policies and measures designed to keep minors off of our platforms... we are always improving our safety efforts and innovating in response to advances in technology and increased understanding of safety-related concerns in the industry."**
>
> **– Round table participant**

During roundtable discussions, industry indicated that they perceive a risk-based approach to be ambitious and complex. Industry participants emphasised that a risk based approach would require a risk assessment or similar to inform industry's actions. From the perspective of industry participants this should include consistent definitions of:

- Threats and potential harm;
- Service features that carry more or less risk;
- Likelihood of threats in the scenario that a child accesses a platform;
- Options for risk mitigation, e.g. methods of age assurance[80]

[79] Please refer to page 47, reference #2
[80] Ibid

Industry felt that case studies are essential for the development and agreement of this risk assessment.[81]

During the VoCO Phase 2 workshops, subject matter experts proposed this being delivered through child safety impact assessments, which would be similar in their approach to data protection impact assessments. An industry participant noted that their company would be concerned about requirements to publicly publish a risk assessment for age assurance. Their approach would be to talk to the government and regulators directly to gather advice and share their assessments, rather than make public their actions to meet potential age assurance requirements.

Platforms Principle #2

As a platform, if I'm going to recognise and protect my child users... *I don't want to be commercially disadvantaged* because my competitors aren't held to the same standard.

Initial industry reaction expressed concern that age assurance and related child safety measures will add friction to user interactions, which may make services less desirable for users and could impact business competitiveness.[82] During workshops with industry specific concerns raised include loss of users, and loss of advertising potential.

During the VoCO workshops with industry, there was further concern that if age assurance became a legal requirement on companies before a commercially viable methodology had been established platforms could respond by banning children. Specifically, there was concern that platforms would choose to ban children from accessing services if it was easier than changing their approach.

One participant, from a platform that provides universal content, stated that age assurance would impact significantly on the availability of universal content and their ability to provide it. Such barriers could prevent the most vulnerable children from accessing positive content, as their parents may not support them with access. Another respondent noted that because their platform provides content designed for children, they already have a high level of age assurance controls in place, but nevertheless would like to improve customer experience (whilst maintaining a high level of user and parental trust) through reduced friction. They do not have the resource to develop tech solutions to make this possible but would like to work with other platforms to achieve this and create a better solution for all.

Several industry participants felt that to maintain service quality for users, age assurance should be required at the "distribution layer" of the internet supply chain – i.e. at the app store and operating system levels, rather than at the individual app or platform level. One participant from a platform popular with children and young people agreed that app stores are key and believed that there is a greater opportunity for action by adopting an incremental approach with app store companies.

During industry roundtable discussions, a participant noted the context of public perception in enacting age assurance. The participant felt that some data sources such as biometric data might be perceived as intrusive by the public, in particular when it was children's data. They felt this may impact on the commercial viability of some methods.

From the VoCO Phase 2 Workshops, VoCO identified the following actions which may facilitate the above principle:

1. All platforms must adhere to the same age assurance processes.
2. Consider that safety is an important factor in the investment management process.
3. Potentially create a coalition or venture capitalist group to champion the technical solutions to VoCO.

[81] Please refer to page 47, reference #2
[82] Ibid

Platforms Principle #3

As a platform, if I'm going to recognise and protect my child users… *I want my liability to recognise the measures I have implemented to protect them* if, despite these, harm still occurs.

A respondent from a 'younger' platform noted that there is concern that government will impose blanket age assurance conditions without recognising platforms' own risk mitigation steps. This respondent stated that they are able to make technical changes more easily than incumbents, and are keen to do that where needed, including developing and trialling solutions without it being government-mandated. In roundtable discussions, respondents highlighted that knowledge sharing and benchmarking mechanisms are vital, both for companies and regulators, and that proactive and constructive engagement should be incentivised.[83]

Digital Parents

Digital Parents' Principle #1

As a digital parent, if I'm going to allow my child to use your platform… *I want peace of mind* that the platforms are protecting my child and they are giving me the information I need to do the same.

A key theme that emerged through VoCO engagement with parents was the opinion that technology companies should be doing more to protect children. When asked directly whether they would be supportive of apps or platforms knowing their child's age and tailoring their online experiences, 18 out of 22 parents were supportive. Overall, parents felt that their children's safety should be a greater priority for companies.[84]

> **Different needs of children at different ages and stages of development should be at the heart of how [platforms] design [their] service.**
>
> **- Age Appropriate Design Code, ICO**

Many of the parents we engaged with indicated that they struggled to keep up with the different sites and services that their children are using and sometimes with the fact that their children moved between different environments (and sometimes between different parents or different placements). As a result, they felt that companies should be doing more at the design stage to keep their children safe and that this should be consistent across platforms. In this situation, parents and carers would not need to assess every new platform their children are using because they would be reassured that internet services are actively trying to prevent harmful content or contact.

> **On three occasions there have been police investigations with girls in our care over the years and every time when the information or evidence they need is on [a social media app] they can't recover the images, or messages or any content. It makes safeguarding these kids incredibly difficult. I think it's irresponsible and dangerous.**
>
> **- Foster Carer**

Digital Parents' Principle #2

As a digital parent, if I'm going to allow my child to use your platform … *I do not want it to be burdensome* because I need to make timely and informed decisions about my child's wellbeing.

[83] Please refer to page 47, reference #2
[84] Please refer to page 47, reference #1

Internet Matters research indicated that parents want a mechanism that facilitates the device rather than inhibits it. The current situation is that parents do not understand how to apply safety settings and what this protects children against. Rapidly developing technology and multiple platforms, each with specific settings of their own, makes this even harder for parents to navigate.[85] Solutions that facilitate the VoCO Manifesto should recognise the time and knowledge pressure on digital parents and have realistic expectations on what they can do without overloading them. As one parent we engaged with explained "parenting is incredibly difficult already without the added pressures of the internet".

During VoCO engagements with digital parents it was felt that a trust mark that is continuously re-assessed, could provide them with the level of assurance required to feel that their children are being safeguarded online.

Digital Parents' Principle #3

As a digital parent, if I'm going to allow my child to use your platform... *I want to know my child's rights are being respected* as a result of the decisions taken by the platforms and myself.

One of the findings of the VoCO engagement with digital parents was that there needs to be more engagement with them about how age assurance technology works and how their children's data can be protected and minimised. Participants felt that it should be clear what data is being shared and how it is being shared. Through workshop conversations, digital parents were initially apprehensive about the potential methods for delivering age assurance, whether biometrics or behavioural. Ambiguity in the process needs to be resolved to assuage privacy concerns.

During these workshops it what was felt that the following would be required to achieve this:

1. Clear terms and conditions that are upheld by the platform;
2. Visibility of the data held;
3. Default safety settings, including means of complaints and user redress if rights are not being respected;
4. Simplified and accessible information about the risks and what is being done to safeguard children; and
5. Tools to help a child user exercise their rights, e.g. easy to delete content or data.

Children

For children the principles focus on them continuing to enjoy the positive benefits of the internet and not feel as though they are being excluded. This relates to both connecting and socialising with peers and the content that they engage with.

Childrens' Principle #1

As a child, if I am going to be honest about my age... *I do not want to feel like I am missing out* because my friends can do things that I cannot.

During focus groups with primary-aged children, there was general support for an age targeted or age banded internet with more appropriate content and interactions with people of a similar age. A key aspect of their internet experience that the children liked and wanted to preserve was their interactions and the fun they had with their friends. However, despite currently using many general audience websites, there was no great desire among the primary-aged group to interact with significantly older children and no desire to interact with or play games with adults.

> **I lied to gain access to the social media I suppose, to talk to my friends, especially when you're 13 and you're joining a new school it was definitely a thing that happened. Everyone joins [social media platforms]. Like a networking thing of who's who, group chats, and everyone new joining and all of that. I think that's why we did that. To gain more social exposure to people.**
>
> **- 18-year-old girl**

[85] Internet Matters, 'Parenting Digital Natives', 2018

In contrast to the children of primary age, in the engagement sessions with older children they tended to express more concern about being restricted from their older friends. In one of these sessions of 12-15 year-olds, the young people expressed concern about a potential restriction to specific age bands for some sites; “I have loads of mates who are 16 and I want to look at their posts".[86]

Through conversations with children in care, the children presented some concerns about potentially being excluded or missing out as a result of age assurance if it were to require them to produce official documentation. One child said that their school knew how old they were, but that their carer did not have official documentation and spoke about the difficulty of going to the cinema without proof of age. The foster carers also talked about how difficult it could be to get hold of official documents for their children. Given that exclusion can happen offline, there were also concerns from these groups that it would also occur online.[87]

It is essential that there are a range of ways for a child’s age to be assured by the platforms to ensure no children are left out or feel excluded. In this respect the ‘walled garden’ approach, where children of a younger age are banded together without older children or adults may not be the most effective approach for many services – albeit there was some support for children’s versions of apps among younger children. Overall, for older children in particular, a more effective and positive approach, might be to tailor services so that they have clearer information and options over their settings for who they want to interact with online and how they want to control and share their content.

Childrens’ Principle #2

As a child, if I am going to be honest about my age... *I want a better experience* that lets me do more rather than less things.

Currently, there is a perceived gap in the market for platforms that are designed for children and are safe but still contain engaging content. Because few exist, and those that do are not of a high quality, children are fairly dismissive of platforms intended just for them. In a focus group of 12-15 year olds, none of the children wanted to be in an online space for just their age group.[88] As stated by one 14 year-old girl, “It wouldn’t be the same [to have an app that knew my age and gave me a different experience to the adult experience I’ve been having]. My mum wouldn’t be able to get in touch”.

> **It does worry me about grown-ups I don’t know contacting me but I want to go on what I want without being restricted.**
>
> - 12 year old boy

However, VoCO found that there is interest in having a safer space, provided the content is perceived as equally engaging. At the primary school age, children liked the idea of having a safer space, but at the same time expressed the desire to have access to the same videos of dances and songs and still be allowed to post videos and play games. This sentiment was reiterated by children in care. For example, 11 out of 16 children in care said they would like sites that are ‘just for kids’ but with good content, not a ‘lite’ version of the grown-up sites. For older children, the concern focused on not wanting to feel excluded from content, as one young person in a mainstream school explained.[89]

> **If it was a thing and people said how old they were, people wouldn’t be as interested because you’d be thinking what’s on the other things? If [social media platforms] did age checks and people started finding out what was on other ages, you’d be wondering what was on there.**
>
> - 12-year-old boy

Through the VoCO Phase 2 workshops, the subject matter experts hypothesised that main sites should be adapted to children rather than creating ‘kids only’ sites. This requires research and engagement with children as to what they define as ‘better.’

[86] Please refer to page 47, reference #1
[87] Ibid
[88] Ibid

Childrens' Principle #3

As a child, if I am going to be honest about my age... *I want to feel safer* because I know I am being protected from the bad stuff that can happen online.

There was particular interest among primary age children in having greater protections online from the things they did not like. The primary age children were forthcoming about things they wanted to be different including wanting less violent content and fewer contacts from unknown adults. This was true to an extent of the engagements with the three older groups of children. For example, the children in care (ages 12-15) expressed interest in being protected online in terms of sites doing more to get rid of 'nasty people' and more control over how their content was shared and removed. One 9 year old girl said in relation to a popular social media app, **"there's not any info on staying safe, only how to use the app but not about staying safer".**

VoCO found that in general, with the older children, their desire for a better internet experience was expressed less explicitly in terms of safety (many of the children and young people were keen to express that they could manage the challenges of the online environment) and more in terms of enhanced controls and better systems. They were more interested in the greater safety and protections that age assurance might provide for their younger siblings or friends. However, they wanted better systems in place for a range of their internet experiences. For example, in relation to reporting, one 15 year-old girl stated, "If you press report on [a social media app], then it gives you a multiple choice, when you do that it says why do you want to report, then it says ok thank you, but no response and they are probably still following you". There was scepticism about the current systems and protection based on their current experience. This was particularly acute in relation to their lack of control over their digital footprint, they wanted better control over how their content is shared and wanted the ability to screen or remove content that they had produced. [1]

7.5 References and Supporting Documents

VoCO Phases 1 and 2 consisted of multiple workstreams examining various aspects of VoCO in depth. Outlined below are the detailed reports that were produced by each of the workstreams and utilised as references throughout this report.

Phase 2 Documents

#	*Phase 2 Output*	*Purpose*
1	Praesidio, "COM116 – WP1.1a: Final Report," 2020	Captures the views of children, parents, carers and teachers as it relates to their online experience and age assurance.
2	J. Shipp, "COM116 – WS1.1b Industry Engagements," 2020	Documents Industry feedback on VoCO proposition and creates an initial point of view about its proportionality, desirability and feasibility.

[89] Please refer to page74, reference #1

3	**Obidos Consulting, "COM116 – WS1.1c Regulatory Engagement Report," 2020**	Documents how regulators approach the task of regulation and the importance of online age verification.
4	**C. Tullo, "COM116 – WS2.1a Standards recommendations," 2020**	Reviews existing standards and frameworks to identify what would facilitate the VoCO proposition and create and overarching ideal future stateand feasibility.
5	**Aleph Insights, "COM116 – WS2.1b VoCO Data Sources Type Taxonomy Guide and Assessment," 2020**	Provides a taxonomic structure for the organisation of data sources that are relevant to the task of verifying children online and assesses their feasibility.
6	**Safehaus., "COM116 – WS2.1d Charging and commercial options," 2020**	Assesses the commercial considerations for potential VoCO solutions.
7	**TrustElevate, "COM116: Tech Trials Report," 2020**	Discusses how TrustElevate was used as a proof of concept to test the feasibility of a potential VoCO solution.

Phase 1 Documents

#	***Phase 1 Output***
8	J. Vertigan, "C081-WS1.2 Market Analysis," 2019.
9	R. O'Connell, "C081-WS2.2 Technical Trials," 2019.
10	O. Vaughan-Fowler, H. King and Z. Hilton, "C081-WS1.1.1 Landscape Mapping," 2019.
11	D. Clarke, "C081-WS2.1 Product Selection," 2019.
12	O. Vaughan-Fowler, H. King and Z. Hilton, "C081-WS1.1.2 Use Cases," 2019.
13	HACKMASTERS, "C081-WS1.3 Task Force Outputs," 2019.
14	GCHQ, "Verification of Children Online (VoCO) Insights and Recommendations Report," 2019

External Sources

15	Unicef, ‘One in Three: Internet Governance and Children’s Rights’, 2016
16	HM Government, ‘Online Harms White Paper,’ 2019
17	Ofcom, ICO, ‘Internet users’ concerns about and experience of potential online harms’, 2019
18	Information Commissioner’s Office (ICO), ‘Age Appropriate Design: A Code of Practice for Online Services,’ 2019. (NIST SP 800-63b)
19	BBC, ‘Social media apps are deliberately addictive to users,’ 2018
20	Internet Matters, ‘2018 Survey’, 2018
21	United Nations, ‘The United Nations convention on the rights of the child’, 1989
22	5Rights, ‘The 5Rights Framework’, 2020
23	Macenaite, M, ‘Consent for processing children’s personal data in the EU: following in US footsteps?’, 2017
24	Internet Matters, ‘Parenting Digital Natives’, 2018
25	HM Government, ‘Keeping children safe in education’, 2019
26	New Zealand Government ‘Digital Identity Trust Framework’, 2019
27	NIST Internal Report, ‘Developing Trust Frameworks to Support Identity Federations’, 2018, (NISTIR) 8149
28	Children’s Commissioner, ‘Life in Likes’, 2018
29	Internet Matters, ‘10 things you need to know about cyberbullying’, 2020
30	IWF, ‘The Dark Side of a Selfie’, 2020
31	NCMEC, ‘2019 Reports by Country’, 2020
32	BBC, ‘Facebook removes 11.6 million child abuse posts’, 2019
33	Internet Matters, ‘Vulnerable Children in a Digital World’, 2019

34	NSPCC, ‘Taming the Wild West Web’, 2019
35	Interactive Schools, ‘How long does it take tech to reach this milestone?’, 2018
36	Europol, ‘Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic’, 2020
37	Express & Star, ‘Girls as young as six sexting during pandemic, cyber safety research suggests’, 2020

7.6 Glossary

A

AI (Artificial Intelligence) - The use of computers to perform tasks normally requiring human intelligence, such as visual and speech recognition, analysis of natural language, and decision-making. Machine learning (qv) is a type of artificial intelligence.

Access-by-Age - Access-by-Age services encompass those which by law should only be accessible to certain age ranges (such as pornographic material or the selling of alcohol).

Age Appropriate Design Code (AADC) - A code of practice for online services published by the Information Commissioner’s Office (ICO) after consultation, on 22 January 2020. The code has been laid before Parliament and is expected to come into force Autumn 2021. The code is based on the relevant provisions of the Data Protection Act 2018 and GDPR.

Age Appropriate Services - Services designed for the age range of its users. For example, when providing a service to younger users it should ensure that appropriate safety features, GDPR concerns, parental consent and moderation are all considered.

Age Assurance - Age assurance is the broad term given to the spectrum of methods that can be used to assure a user’s age online. Age assurance allows companies and users to jointly choose from a range of measures that are appropriate to the specific risks posed and their service needs. The selected methods may rely on different sources of data, which may have different privacy implications and cost models.

Age Checking - A way of performing age assurance that preserves the individual’s privacy by checking only a single attribute of their identity, in this case their age. The response to an age check, for example whether a user is over 16 years of age, is yes/no, and can be passed as an Attribute Token. A trust score can also be provided by the age check service, which indicates the level of trust that can be placed in the response.

Age Check Exchange - Online internet gateway for age check providers and relying parties to access user asserted, permissioned, and verified attributes.

Age Check Practice Statement - A document describing the operational practices and procedures of an age check service.

Age Check Provider - An organisation responsible for all the processes associated with establishing and maintaining a subject’s identity attributes.

Age Confidence - A measure which determines how certain a platform is about the age of their individual users. The age confidence level needed by a platform is based on the assessment the platform has made on the degree of risk posed to a child by the service.

Age Range - The right of access to goods or services based on age or age band.

Age Verification - Age verification is a form of age assurance where a user’s age is established through a full identity verification process to a high level of confidence. Currently, age verification is most commonly used to help businesses meet legislative requirements concerning age-restricted products and services by restricting access to users who cannot provide officially held evidence that they are over 18 years of age.

Anonymisation - A process where data is permanently rendered anonymous in such a way that the data subject is no longer identifiable and is therefore not personal data.

Attribute - Information about a subject which relates to an individual.

Attribute Token - A token which is stored and passed in a digital form, and can carry only the attributes (e.g. age, or age band) that a user is required to provide to the requesting service or platform called tokenised age checking.

Authentication - The process of identifying a previously registered user.

Authoritative source - A source, through official status or reputation, that can be trusted to provide accurate data, information and/or evidence that can be used to prove age.

B

Biometric Data - Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that person (or an element of that person's identity such as their age). Includes fingerprint scanning, facial recognition and voice identification.

C

Child - Under GDPR a child means anyone under the age of 18 in accordance with the UN Convention on the Rights of the Child. Age range is not a complete guide to the interests, needs, behaviours and evolving capacity of each child. To help assessment the ICO uses the following age ranges and developmental stages as a guide:

- 0 - 5: pre-literate and early literacy
- 6 - 9: core primary school years
- 10-12: transition years
- 13-15: early teens
- 16-17: approaching adulthood

Community of interest - A group of parties, signed up to a trust framework, who wish to obtain or verify user identity attributes.

Credential - An assertion that can be presented by an age check service to a relying party to authenticate the user and can be reused.

D

Data Protection Impact Assessment (DPIA) - A defined process to help identify and minimise the data protection risks of a service with particular reference to the specific risks to children likely to access services which process their personal data. DPIAs are core to document compliance and meet the accountability obligations under GDPR and demonstrate the adoption of a 'data protection by design' approach as part of the Age Appropriate Design Code.

Duty of Care - Duty of care is described in the Online Harms White Paper (OHWP) as part of the new regulatory framework put forward for online harms that will help to make companies take more responsibility for the safety of their users, and tackle harm caused by user-generated content or behaviour on their online services. Compliance with this duty of care will be overseen and enforced by an independent regulator.

Data processing - Defined widely and includes collection, storage, use, recording, disclosure or manipulation of data whether or not by automated means.

F

Federated attribute exchange - The means of linking an individual's attributes, stored across multiple distinct systems or domains while keeping their internal autonomy intact and secure.

G

GDPR - General Data Protection Regulation incorporated into UK law in the Data Protection Act 2018 and applies in the UK from May 18, 2018. After EU exit day, references to GDPR mean the equivalent provisions in UK GDPR. GDPR applies in the UK in the same way as it did before EU exit day. At the end of the implementation period (end 2020), the default is that GDPR and the Age Appropriate Design Code remain in effect.

Grounds for processing - The lawful basis for processing personal data – consent; contract; legal basis; vital interests; public interest; legitimate interest.

I

Identity Information Provider - Entity that makes available identity information.

Information Commissioner's Office (ICO) - The UK independent regulatory body that upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

O

Officially Provided Information - Data that derives its status, and therefore its authority, from being controlled, collated, collected or maintained by government, a regulator or other official source.

P

Parent - A parent exercises parental responsibility and means the person(s) who, according to the law in the child's country of residence, has the legal rights and responsibilities for a child that are normally afforded to parents. This will not always be a child's 'natural parents' and parental responsibility can be held by more than one natural or legal person.

Parental Consent - Consent from a person holding parental authority over children under 16.

Personal Data - Any information relating to the private, professional or public life of a living person that can be used directly or, when combined with any other information, indirectly to identify the person.

Platform - A group of technologies used as a base upon which other applications, processes or technologies are developed. In personal computing, it is the basic hardware (computer or mobile device) and software (operating system) on which software applications can be run.

Privacy Notice - A published notice informing individuals how their personal data is going to be used, the lawful basis on which it is being used and their rights when their data is provided, collected and processed.

Profiling - Any form of automated processing of personal data that uses the data to evaluate certain personal aspects relating to an individual, in particular that analyses or predicts aspects relating to that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation - A process undertaken to ensure that no personal data can be attributed to an individual without the use of additional information, where identifying fields within a data record are replaced by one or more artificial identifiers or pseudonyms.

R

Relying Party - Organisation relying on results of an online age check to establish the age-related eligibility of an individual for the purpose of a transaction.

S

Special Category Data - Personal data that needs more protection because it is sensitive and includes racial origin, sexual orientation, political or religious views, trade union, health, genetic or Biometric Data.

T

Trust - Degree to which an entity has confidence in the accuracy, integrity and reliability of age checking processes.

Trust Framework - An underlying legal structure of standards and policies that defines the rights and responsibilities of participants in an identity ecosystem, specifies the rules that govern their participation, outlines the processes and procedures to provide assurance, and provides the enforcement mechanisms to ensure compliance.

V

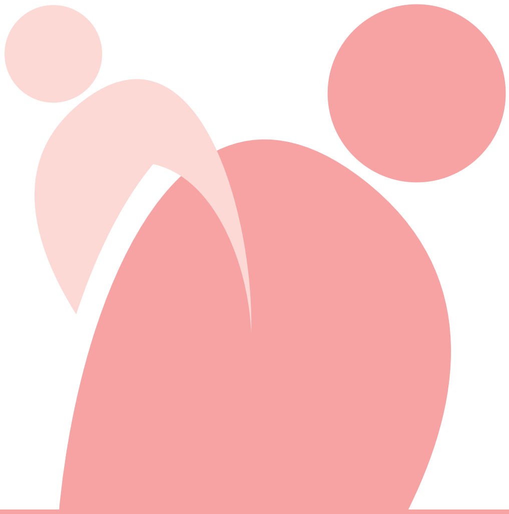
Verification - The process of establishing the truth, accuracy, or validity of a piece of information. See Age verification.

Verified Parental Consent - The ability for a parent and child to prove their relationship to a platform so that the platform can empower the parent to provide consent and controls to guide their child's online experience.

VoCO

(Verification of Children Online)

Phase 2 Report



November 2020