

Call for evidence response form

Please complete this form in full and return to os-cfe@ofcom.org.uk

Title

Second phase of online safety regulation: Protection of children

Full name

✂

Contact phone number

✂

Representing (select as appropriate)

Organisation

Organisation name

Fujitsu Services Ltd

Email address

✂

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see [Ofcom's General Privacy Statement](#).

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? (select as appropriate)

Nothing

Your response: Please indicate how much of your response you want to keep confidential (select as appropriate)

None

For confidential responses, can Ofcom publish a reference to the contents of your response? (select as appropriate)

Yes

Your response

Question 1: To assist us in categorising responses, please provide a description of your organisation, service or interest in protection of children online.

Is this a confidential response? (select as appropriate)

No

Fujitsu is a global Information, Communication and Technology (ICT) company that has developed a range of solutions that digitally verify the age of individuals wanting to access age restricted content, products and services that are available online or on-premises.

Organisations integrate our technology and solutions into their systems to introduce age controls that protect minors from harm by preventing them from accessing age restricted content, products, and services.

Our technology and solutions integrate with online content and service providers enabling them to determine the level of access and entitlement an individual may have based on their age via a secure challenge/response mechanism.

The system requires an individual to use their mobile phone to initially register and then verify themselves when accessing online content and services.

Registration is quick, simple, and secure and requires an individual to download an app onto their mobile phone and then digitally scan a recognised form of photo identity. Then uses biometric matching technology to confirm the identity of the individual with the identity documents and create a secure credential that is stored on the phone.

Verification takes less than 2 seconds and is required when an individual wants to access age restricted content and services. To verify, an individual opens the app and scans their face to biometrically confirm their identity. They then scan a challenge QR code presented by the online content and service provider and the resulting age is passed from the individual's mobile phone to the service provider and access provided, if permitted.

No Personal Identifiable Information (PII) is shared with the service provider and the individual's personal information remains on the phone in a secure encrypted state. The individual remains anonymous to the service provider and is tracked by a unique User ID.

The unique User ID can be used to block an individual from accessing the service providers site, should the individual contravene the sites acceptable use policies.

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 3: What information do services have about the age of users on different platforms (including children)?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 4: How can services ensure that children cannot access a service, or a part of it?

Is this a confidential response? (select as appropriate)

No

Fujitsu believes that technology can be implemented by site operators that would effectively prevent individuals accessing, viewing, or obtaining age restricted content, products, or services, and prevent minors from harm.

Age Assurance technology that enables a site operator to verify the age of an individual can be used to restrict the content, products, and services that an individual is entitled to access and act against individuals that create and share content that contravenes a sites acceptable use policy, allowing site operators to block both the account and the individual, preventing the further publication of harmful content from that account.

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Is this a confidential response? (select as appropriate)

No

Our technology and solutions integrate with online content and service providers enabling them to determine the level of access and entitlement an individual has based on their actual age. The system uses a secure challenge/response mechanism to confirm that an individual is who they say they are.

Age Verification services vary in price, most have a license cost and per transaction verification charge.

Most Age Verification service providers use SaaS based services, that are liable to unexpected downtime. Any service outage will mean that Age Verification services will be unavailable to the online content service provider requiring site operators to fall back on less robust controls or risk impacting the service provider's revenue.

Our solution does not incur a per transaction cost to the service provider, allowing online content and service providers to understand their costs upfront.

Our system of Age Verification does not have a SaaS component and is designed to be fault tolerant and is therefore not liable to unexpected downtime and/or temporary relaxation of controls by a service provider.

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?¹

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

¹ See A1.2 to A1.3 of the call for evidence for more information on the indicative list of harms to children.

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

Is this a confidential response? (select as appropriate)

No

Technology can assist online content and service providers in taking significant steps towards protecting minors from accessing age restricted content and services and better manage and control individuals that post inappropriate content that either may be accessible to minors and/or contravene the sites acceptable use policies.

Online content and service providers are responsible for the content visible on their platforms and controlling and restricting who can access it.

It is common for online service providers to use account registration and login controls to access their site, but it is recognised that such controls can be exploited by individuals falsifying information during the account registration process to mask their identity or circumvent age controls.

Further, account-based information can be exploited and shared with unknown third parties to gain access to restricted content, products, and services.

Online content and service providers need to adopt methods that can verify the individual rather than solely the account.

Adoption of such technology will allow service providers to:

- Validate the registered owner of an account is who they claim to be
- Implement robust age verification controls
- Control account access to age-appropriate content, products, and services, including interactions between registered site members
- Remove fake accounts

By adopting methods that make the end user responsible for presenting valid credentials to verify they are who they claim to be, online content and service providers can maintain regulatory compliance, improve audit and traceability of content posted online, and allow restrictions to be enforced based on the individual accessing, viewing, and creating content rather than the account they are using.

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Is this a confidential response? (select as appropriate)

No

Fujitsu believes that technology can be implemented by site operators that would effectively prevent individuals accessing, viewing, or obtaining age restricted content, products, or services, and prevent minors from harm.

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Technology and solutions that verify an individual against a specific registered account provide site operators with greater controls than existing systems that rely on basic self-attested account registration and login controls.

Technology that enables a site operator to verify the age of an individual can be used to restrict the content, products, and services that an individual is entitled to access and act against individuals that create and share content that contravenes a sites acceptable use policy, allowing site operators to block both the account and the individual, preventing the further publication of harmful content from that account.

The application of technology to verify an individual can be deployed specifically for a site operator and/or a broader industry approach taken. Where a broader industry approach is considered, technology to digitally verify an individual could potentially be adopted and supported by a scheme operator such as PASS CO, a government backed proof of age standards scheme, to support wider national requirements for digital age verification.

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

Is this a confidential response? (select as appropriate)

No

Our technology and solutions integrate with online content and service providers enabling them to determine the level of access and entitlement an individual has based on their actual age.

The system uses a secure challenge/response mechanism to confirm that an individual is who they say they are. The system requires an individual to use their mobile phone to initially register and then verify themselves when accessing online content and services.

The individual's identity, date of birth, and a biometric match is undertaken during the initial registration process to create a secure credential and it is this information that is biometrically verified each time the individual accesses the service provider's online site.

During the verification process the system shares the recorded age and a Unique Identifier for the individual with the site operator. The site operator uses the verified age provided by the system to serve content and set access entitlements for the individual's online account.

The Unique Identifier is linked to the individuals online account, and should the account contravene the sites acceptable use policy it can be blocked by the site operator.

The system provides many benefits that protect individuals from harm and site operators from the impact of illegal content.

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

- Age verified access can prevent minors from accessing age-appropriate content and services
- Interaction and content sharing between accounts can be controlled
- Attribution of content between individuals and accounts can be monitored and controlled
- Individuals and accounts can be blocked from accessing the site, if in breach of site policy.
- An account cannot be shared with another individual or group
- Restricts the use of robotic/ghost accounts used to generate automated content as an individual is required to verify account access.

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 19: With reference to content that is harmful to children, how can a service mitigate any risks to children posed by the design of algorithms that support the function of the service (e.g. search engines, or social and content recommender systems)?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

Is this a confidential response? (select as appropriate)

No

Fujitsu believes that improvements can be made to content moderation if better controls are implemented to verify an individual against a specific registered account that is used to access and publish content on a site.

It is common for online service providers to use account registration and login controls to access their sites, but it is recognised that such controls can be exploited by individuals falsifying information during the account registration process to mask their identity or circumvent age controls.

Further, account-based information can be exploited by individuals or groups to create fake accounts and post content that can be inappropriate, illegal, or contravene the sites acceptable use policy.

To prevent this, site operators need to implement technology that creates a direct relation between an individual and their registered account, and that requires an individual to verify that they are who they say they are when using that account. This will enable site operators to:

- Verify the individual accessing a site
- Trace published content to a specific account and individual
- Block site access at an individual and account level where the sites acceptable use policy has been contravened
- Prevent the registration of shared and fake accounts.

Therefore, if better controls are implemented to verify an individual against a specific registered account it would enable online content and service providers to better moderate content, improve user attribution for published content, and help tackle the prevalence of fake accounts that are used as a common vehicle to publish inappropriate content.

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 22: How are human moderators used to identify and assess content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 23: What training and support is or should be provided to moderators?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?

Is this a confidential response? (select as appropriate)

No

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 25: In what instances is content that is harmful to children, that is in contravention of terms and conditions, removed from a service or the part of a service that children can access?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 26: What other mitigations do services currently have to protect children from harmful content?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?

Is this a confidential response? (select as appropriate)

No

Fujitsu provides online content and service providers with a system to age verify individuals accessing sites containing age restricted content, products, and services.

Individuals that want to access sites protected by our technology are required to register prior to accessing the site(s).

To register an individual needs a mobile phone, a recognised photo identity containing their date of birth, and to download the site app.

The system authenticates the individual using a biometric algorithm to cross reference against their ID (to ensure they are who they say they are) and verify their age, thus removing the possibility of fake or borrowed ID's being used.

The online age controls provided by the system can be embedded into an existing app or online platform. Access to the site is performed using a challenge/response mechanism.

The individual uses their mobile phone to verify their identity using the biometric matching capability within the installed app and is then asked to scan a unique time sensitive QR code presented online by the site operator. On reading and validating the QR code the mobile phone securely passes the individual's age and a Unique Identifier to the site operator and access is granted with the appropriate age restrictions set.

The Fujitsu age verification system does not require an individual to register with an online content and service provider to access systems protected by Fujitsu but does require the individual to have registered themselves using their mobile phone prior to accessing the site.

Question 28: Other than those covered above in this document (the call for evidence), are you aware of other measures available for mitigating the risk, and impact of, harm from content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.