Information Commissioner’s Office

# Consultation:

# Age Appropriate Design code

Start date:15 April 2019

End date: 31 May 2019

Information Commissioner’s Office

# Introduction

The Information Commissioner is seeking feedback on her draft code of practice Age appropriate design - a code of practice for online services likely to be accessed by children (the code).

The code will provide guidance on the design standards that the Commissioner will expect providers of online 'Information Society Services' (ISS), which process personal data and are likely to be accessed by children, to meet.

The code is now out for public consultation and will remain open until 31 May 2019. The Information Commissioner welcomes feedback on the specific questions set out below.

Please send us your comments by 31 May 2019.

**Download this document and email to**:
ageappropriatedesign@ico.org.uk

**Print off this document and post to:**
Age Appropriate Design code consultation
Policy Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the consultation please telephone 0303 123 1113 and ask to speak to the Policy Engagement Department about the Age Appropriate Design code or email ageappropriatedesign@ico.org.uk

## Privacy statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public or a parent). All responses from organisations and individuals responding in a professional capacity (e.g. academics, child development experts, sole traders, child minders, education professionals) will be published. We will remove email addresses and telephone numbers from these responses but apart from this, we will publish them in full.

For more information about what we do with personal data, please see our privacy notice.

# Section 1: Your views

**Q1.** Is the '**About this code'** section of the code clearly communicated?

Yes

On a general note: Facebook welcomes the opportunity to respond to this consultation. The protection of children's personal data is an incredibly important issue, and Facebook fully supports measures to keep children safe online. We aim to provide a service that is safe and privacy-protective for all users, and in particular for young people. We are committed to continuing our engagement with the Information Commissioner's Office to find practical ways to enhance transparency and privacy controls for young people. We agree with the ICO about the importance of internet access in supporting children's development, including as an educational resource, communication with friends and family, and engaging with valuable tools and services. We welcome the opportunity this consultation provides to address the important issues of digital literacy and digital inclusion.

We also appreciate the opportunity to share concerns and constructive feedback about some aspects of the Code. Notably, we strongly suggest that the ICO employ a risk-based approach to assessing the suitability of personalised services (also known as "profiling") for children. Many modern Internet services and products are, at their core, personalised in nature— meaning they offer consumers rich, tailored content and experiences based on their preferences and activity on and off the service. The vast majority of personalisation is key to consumers' desire to use the service in the first place, and is not intrusive from a privacy point of view. We encourage the ICO to focus on personalisation and profiling that is likely to cause harm to children, such as automated decisions regarding education, employment, and the like.

We also note with concern that some companies may be required to verify the age of their users, potentially through the use of identity documents. Any solution which aims to protect young people online needs to be aware that millions of people often don't have a way to prove their age or identity. Even those who can prove their age or identity would be asked to provide far more detailed personal data than would otherwise be required to use certain services. However, we welcome the opportunity to work with the government, civil society and others in industry on alternative solutions. For example, artificial intelligence may offer one possible way to accurately identify younger users of services without requiring the storage of official documents, although more work needs to be done in this space.

Generally, the 'About this code' section is clearly communicated. However, we would like highlight two potential concerns:

Some aspects of the code concern issues that also fall into the scope of the UK Government's Online Harms White Paper, such as screen addiction. The White Paper is currently undergoing public consultation (https://www.gov.uk/government/consultations/online-harms-white-paper), with a deadline of 1st July 2019. Facebook will also respond to the White Paper consultation, and we express our hope that the ICO seek alignment with the UK Government both on those issues where there may be overlap, as well as on the timeline for finalising the Code.

We would also like to highlight that the GDPR does not grant Member States the general freedom to establish specific rules for the processing of children's data - except in regards to allowing member states to lower the consent age threshold between 13 and 15 (Article 8).

Therefore, any interpretation and enforcement of the code should be in line with the GDPR requirements.

**Q2.** Is the '**Services covered by this code'** section of the code clearly communicated?

Yes

This section notes that "[u]nder the GDPR one-stop-shop arrangements, if you have a lead supervisory authority other than the ICO and you do not have a UK establishment, this code will not apply." Facebook is subject to the jurisdiction of the Irish Data Protection Commission (DPC) as its lead supervisory authority pursuant to Article 56.1 of the General Data Protection Regulation (GDPR). However, we are grateful for the opportunity to submit comments on the draft Code and hope to share our experience providing safe and privacy-protective services for children.

## Standards of age-appropriate design

Please provide your views on the sections of the code covering each of the 16 draft standards

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

**2. Age-appropriate application:** Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

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

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

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

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

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

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

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

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

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

**12. Nudge techniques:** Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off privacy protections, or extend use.

**13. Connected toys and devices:** If you provide a connected toy or device ensure you include effective tools to enable compliance with this code

**14. Online tools:** Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

**15. Data protection impact assessments:** Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

**16. Governance and accountability:** Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code

**Q3.** Have we communicated our expectations for this standard clearly?

| 1. **Best interests of the child** |
|---|
| Yes<br>☐ Facebook is committed to providing services that reflect the best interest of young people who use them, in coordination and consultation with parents, regulators, policymakers, and civil society experts. |

☐ We would encourage the ICO to work with industry, child development experts, and others to create a more detailed balancing test to weigh the various interests of the child, and which can be appropriately operationalised by companies. This balancing test could, for example, draw on the legitimate interests balancing test under the GDPR.

☐ There may be occasions where the child's right to privacy may be in tension with their right to free expression or association, or where both these rights may be in tension with other standards in the Code. As the Code recognises in Standard 10, "Parental Controls," such controls "also impact upon the child's right to privacy as recognised by article 16 of the [UN Convention on the Rights of the Child (UNCRC)] and on their rights to association, play, access to information and freedom of expression." In addition, the Code recognises that on some occasions, "the best interests of the child have to be balanced against other interests . . . [f]or example the best interests of two individual children might be in conflict, or acting solely in the best interests of one child might prejudice the rights of others."

☐ In addition, parents play a pivotal role in supporting the development of their children and determining what is best for them. As we noted in our previous submission to the ICO, Article 5 of the UNCRC emphasises the need to respect the responsibilities, rights and duties of parents, extended family members or legal guardians to provide the appropriate direction and guidance in the exercise by the child of the rights recognized in the UNCRC. It is therefore essential that the code fully accounts for the role of parents who are primarily responsible for empowering and supporting their children.

☐In many instances the parent is best placed to support the development and best interest of the child, and it is the responsibility of the ISS to empower parents to guide their children's online activity.

**2. Age-appropriate application**

No

☐ Facebook fully supports and shares the ICO's goal of "ensur[ing] that online services likely to be accessed by children are appropriate for their use and meet their development needs." We would like to provide feedback to help achieve this shared goal in a manner that doesn't inadvertently preclude children and young people from accessing the internet, or otherwise unnecessarily impairing their online experience or impinging on their rights to freedom of expression or association.

□ On age ranges:

□ We appreciate the guidance of the ICO on age ranges, and we would like to work with the ICO and other regulatory bodies to better understand protections suitable to these age ranges. We implement robust privacy and safety measures to protect teenagers between 13 and 17 on our services.

□ Our conversations with parents, parenting groups and experts also suggest many children under 13 have a strong interest in communicating with their peers and otherwise accessing online services, and so there is a need to provide a more safe and positive experience for these children. We have collaborated with child development and other experts to develop Messenger Kids, a kid-friendly messaging service for children under 13 that accounts for their different developmental. We've provided further detail and examples in the comment below.

□ On age verification mechanisms:

□ Facebook aims to provide a service that is safe and privacy-protective for all users, and in particular for young people. In order to use Facebook you must be at least 13 years of age, as set out in our Terms of Service: https://www.facebook.com/legal/terms.

□ We all have a responsibility to try to ensure people using online services are the appropriate age. This is genuinely a complex challenge that spans across many online services.

□ However, we note with concern that some companies may be required to verify the age of their users, potentially through the use of identity documents. Any solution which aims to protect young people online needs to be aware that millions of people often don't have a reliable way to prove their age or identity. Even those who can prove their age or identity would be asked to provide far more detailed personal data than would otherwise be required to use certain services. However, we welcome the opportunity to work with the government, civil society and others in industry on alternative solutions. For example, artificial intelligence may offer one possible way to accurately identify younger users of services without requiring the storage of official documents, although more work needs to be done in this space.

□ More specifically, we recognise the need for a multi-stakeholder discussion in relation to this point and welcome the ICO's initiative to "support work to establish clear industry standards and certification schemes to assist children, parents and online services in identifying robust age verification services which comply with data protection standards," in particular concerning what would constitute "robust age verification" mechanisms. We would encourage the ICO to initiate multi-stakeholder discussions and workshops so its guidance can be adapted to each industry.

□ Facebook already utilises a number of ways to ensure users are the appropriate age, and we are committed to finding additional ways we can further minimise the number of young people who access our platforms under the age of 13. We've provided further detail and examples in the comments below.

□ Finally, it's important to underscore that, when assessing any approach regarding age verification and privacy controls that the protection of minors is not (and cannot be) holistically regulated in the GDPR. The GDPR only refers to the specific case of processing activities of children's personal data (i) conducted in the context of an ISS addressed to children between 13 and 16 years old (depending on the relevant Member State choice); and (ii) which rely on consent as legal basis. Only in this specific scenario (i.e., ISS addressed to children of a certain age and consent being the legal basis selected to the processing activity at hand), parental/alternative guardian consent is required. Other data processing activities may also rely on other legal basis, such as the execution, performance and enforcement of a contract, the protection of the individual's vital interests, the compliance with a legal duty, the protection of a public interest, etc.

**3. Transparency**

Yes

□ The use of communications technologies and online services form part of the everyday lives of children, particularly between the ages of 13-18. This is why it is so critical for companies to ensure they communicate clearly about their services to children. As recognized by the ICO, it's best practice to do so by providing several layers of information ('bite-sized' information) in various formats, which will relate to the children's level of development. Below we provide some examples of how we do this at Facebook.

□ There is tension between providing the level of detail required by the GDPR (e.g. Articles 13 and 14) and informing different age groups in a simple and comprehensible manner. Over-simplifying the language might create the risk of underplaying or obscuring the companies' compliance with the GDPR.

□ We believe that transparent communication with any data subject, including children, should achieve the following objectives:

□ Explain data processing and data protection rights using clear and simple language.

□ Deploy the most effective methods and channels for delivering those messages. To understand which methods and channels are the most effective for this audience, companies can explore employing user testing, evaluation, and refinement based on feedback prior to wider deployment.

□ However, we still have some concerns in relation to how the ICO and other regulators will enforce the GDPR requirements in this area. We believe that the ICO could provide further clarity in relation to this point, as we outlined in our responses below.

**4. Detrimental use of data**

No

☐ The ICO explains that 'detrimental use of data' means “data that is obviously detrimental to children’s physical or mental health and wellbeing or that goes against industry codes of practice, other regulatory provisions or Government advice on the welfare of children.” The ICO also advises that “You should take particular care when profiling children, including making inferences based on their personal data, or processing geo-location data.”

☐ An example of codes of practice provided is the UK Committee of Advertising Practice (CAP)'s guidance on online behavioural advertising. We believe that it is not clear whether, by giving this as an example, the ICO is implying that behavioural advertising practices will be considered as a detrimental use of children's data in general. We would welcome further clarifications on this point.

☐ The GDPR does not prevent companies from processing data from children for behavioural advertising practices. However, Recital 38 specifies that “specific protection should (...) apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child”.

☐ We would also welcome further examples from the ICO on when uses of children's data would be detrimental to them, and whether the ICO believes that companies can mitigate these risks if they submit these processing activities through DPIAs.

**5. Policies and community standards**

Yes

If NO, then please provide your reasons for this view.

**6. Default settings**

No

☐ We agree with the ICO that privacy-protective default settings can be an important way to provide special protections for children's personal data and children's safety online.

☐ The ICO explained that whenever the organisation decides not to apply 'high privacy' settings by default, it needs to “demonstrate that there is a compelling reason for a different setting taking into account the best interests of the child.”

☐ We would like to note that 'high-privacy' settings by default will also depend on the very nature of the service. For example, the audience for children's posts on Facebook is by default their “friends”, which is the most limited of the standard Facebook audience settings. Setting this audience as “only me” by default would undermine the general purpose of a user posting on her timeline, which is to share content with friends.

☐ It's also important to note that many modern internet services are, by their very nature, personalised. Turning off personalisation by default would fundamentally change the service on offer, and therefore should be excluded from this section.

☐ We would also welcome further explanations on the meaning of 'compelling reason' and what kind of assessment test organisations should take in order to demonstrate the reasoning behind this 'compelling reason'.

☐ Organisations should incorporate the principles of data protection by design and by default at early stages of the development their products and services, in particular when these are offered to children. Key considerations include whether children might need simpler explanations to understand their own choices, and how to apply data minimisation in relation to the collection of children's data.

☐ At Facebook we have applied by default settings to children's accounts designed to keep them safe (see below for more details).

☐ We look forward to further debate between industry, civil society and regulators, as well as regulatory guidance, on other measures that could be applied to incorporate the principles by design and by default to online services offered to children.

**7. Data minimisation**

No

☐ The ICO describes data minimisation as “collecting the minimum amount of personal data that you need to deliver an individual element of your service. It means you cannot collect more data than you need to provide the elements of a service the child actually wants to use.” We would welcome further explanations on what would constitute a service that 'the child actually wants to use' and how the ICO would advise organisations to measure this.

☐ It should also be noted that, for many services, personalisation is actually the core of the service on offer. We agree that organisations should be clear if this is the case.

**8. Data sharing**

Yes

If NO, then please provide your reasons for this view.

**9. Geolocation**

Yes

If NO, then please provide your reasons for this view.

**10. Parental controls**

Yes

If NO, then please provide your reasons for this view.

**11. Profiling**

No

☐ We strongly suggest that the ICO employ a risk-based approach to assessing the suitability of personalised services (also known as "profiling") for children. Many modern Internet services and products are, at their core, personalised in nature— meaning they offer consumers rich, tailored content and experiences based on their preferences and activity on and off the service. The vast majority of personalisation is key to consumers' desire to use the service in the first place, and is not intrusive from a privacy point of view. We encourage the ICO to focus on personalisation and profiling that is likely to cause harm to children, such as automated decisions regarding education, employment, and the like.

☐ The ICO explains in the code that "Because profiling can be used to serve a wide range of purposes it is particularly important to be clear about the purposes for which your service uses personal data to profile its users, and to differentiate between them. Catch-all purposes, such as 'providing a personalised service' are not specific enough." We believe that this statement is clear in what concerns personalisation as an aspect of the online service provided. However, in some cases personalisation consists of the core of the service provided-- that is, the service per se.

☐ Where the online service consists of personalisation - for instance, personalisation of content such as in the case of Facebook - the purpose for profiling would inevitably be the provision of the service for which children signed up to. Further details about the description of profiling used in this context would therefore be linked to the description of services - e.g. to personalise the content that is displayed on the user's timeline, friend recommendations and others.

☐ We would welcome further explanations from the ICO on how to be clear about the purposes for which your service uses personal data to profile its users towards children, when profiling is linked to the provision of online services. In particular, we would welcome clarifications as to whether the ICO would consider describing the service not enough, and

| |
|---|
| what level of information the ICO would recommend ISS provide concerning profiling in these cases. |
| **12. Nudge techniques** |
| Yes<br>If NO, then please provide your reasons for this view. |
| **13. Connected toys and devices** |
| Yes<br>If NO, then please provide your reasons for this view. |
| **14. Online tools** |
| Yes<br>☐ We agree that the ICO has clearly communicated their expectations in relation to this standard. However, we would welcome guidance from the ICO also in relation to what instances should parents/guardians be able to exercise data protection rights on behalf of their children.<br>☐ We believe children should generally be able to exercise their privacy rights autonomously at least with regard to online services like Facebook.<br>☐ The approach may vary by sector, and may depend on national laws. In the context of Facebook's services where children are 13 or older, we believe the child should retain the sole ability to exercise her or his privacy rights. Consistent with Article 16 of the UN Convention on the Rights of the Child ("No child shall be subjected to arbitrary or unlawful interference with his or her privacy [...] or correspondence," https://www.unicef.org.uk/what-we-do/un-convention-child-rights/), children's private communications and activity on the Internet should only be accessible upon request of the child.<br>☐ However, in exceptional circumstances - where the safety of the child is potentially at risk - the right to access private content may be extended to a parent or guardian. |
| **15. Data protection impact assessments** |
| Yes<br>If NO, then please provide your reasons for this view. |
| **16. Governance and accountability** |
| Yes<br>If NO, then please provide your reasons for this view. |

**Q4.** Do you have any examples that you think could be used to illustrate the approach we are advocating for this standard?

1. **Best interests of the child**

Yes

☐ At Facebook, we work to ensure the best interests of the child through a variety of methods, including educational resources, tools and controls, and partnerships with child experts. For example, these include:

☐ Educational messages and resources from Facebook related to privacy, security and safety, such as:

☐ Safety Center (https://www.facebook.com/safety): We launched our new Safety Center in 2017 (https://www.facebook.com/fbsafety/videos/1133567856681051/). The Safety Center is one tool we use to help people feel safe and supported on our platform. It walks people through the tools we offer to control their experience on Facebook, as well as numerous tips and resources. It is now mobile friendly, available in over 60 languages, includes step by step videos and resources from about 75 partners around the world.

☐ Youth Portal (https://www.facebook.com/safety/youth): In 2018, we launched a new youth portal with resources for teens and tweens to empower them with information on the tools and policies they have for staying safe on Facebook as well as advice from their peers on a range of topics including managing negative experiences. https://newsroom.fb.com/news/2018/05/the-facebook-youth-portal-and-our-ongoing-work-with-teens/

☐ Parents Portal (https://www.facebook.com/safety/bullying/parents): In 2016, we launched a new "Parents Portal" where caregivers can come to learn some of the basics about Facebook, get tips on how to start a conversation about online safety with their children, and access external expert resources. The portal responds to feedback we have received from parents for more education around our safety policies, tools and resources. And just like our new Safety Center, one of its key strengths is the access it offers to external expert safety partners. We also have a Parents Portal on Instagram: https://wellbeing.instagram.com/parents

☐ Bullying Prevention Hub (https://www.facebook.com/safety/bullying): Developed in partnership with the Yale Center for Emotional Intelligence, the Bullying Prevention Hub is a resource for teens, parents and educators seeking support and help for issues related to bullying and other conflicts. It offers step-by-step plans, including guidance on how to start some important conversations for people being bullied, parents who have had a child being bullied or accused of bullying, and educators who have had students involved with bullying.

☐ Digital Literacy Library (https://www.facebook.com/safety/educators): In 2018, we launched a resource for educators looking to address digital literacy and help these young people build the skills they need to safely enjoy digital technology. Developed for educators of youth ages 11 to 18, the ready-to-use lessons in the Library are drawn from the Youth and Media team at the Berkman Klein Center for Internet & Society at Harvard University, which has made them freely available worldwide under aCreative Commons license (https://dlrp.berkman.harvard.edu/about). https://newsroom.fb.com/news/2018/08/digitalliteracylibrary/

☐ Transparency measures and privacy tools and controls:

☐ General easy to understand information about our service: We believe that being transparent in a clear, plain and comprehensible way is important, and we apply this principle across our service and for our whole user base. Both adults and children benefit from the breadth of simple and clear cut information we provide.

☐ For instance, we have updated our Data Policy (Privacy Policy) in recent years to use more simple, clear language and to provide a more intuitive, layered approach to accessing the information: https://www.facebook.com/policy.php

☐ We've also created Privacy Basics, where users can learn more about sharing, selecting audiences, their visibility, relevant reporting channels etc. Privacy Basics also includes important sections about ads, security and safety: https://www.facebook.com/about/basics.

☐ We have created a dedicated "About Ads" section that includes information about how Facebook collects and uses data to provide relevant ads: https://www.facebook.com/ads/about/?entry_product=ad_preferences.

☐ In-product notice: in addition to our privacy notice and the sources listed above, Facebook provides in-line education messaging adjacent to the setting, which children will read every time when they change their settings.

☐ Our Time Spent tools are another opportunity to foster conversations between parents and teens about the online habits that are right for them and to help make time spent on Instagram and

Facebook intentional, positive and inspiring: https://newsroom.fb.com/news/2018/08/manage-your-time/

☐ Partnerships such as our major anti-bullying commitment (https://diana-award.org.uk/news/anti-bullying/facebook-partnership/). In October 2017, Facebook - in partnership with The Diana Award and Childnet International - offered every secondary school in the UK a trained digital safety ambassador. As many as 26,200 secondary school students and 2,000 teaching staff from 2,400 schools across the UK could be trained as Anti-bullying Ambassadors or Digital Leaders over the next two years. Facebook has spent over a decade developing innovative safety tools, products and programmes to keep young people safe online. This major new commitment ensures that this pioneering work is being felt both inside and outside the classroom.

☐ Our dedicated commitment to supporting vulnerable young people with a range of resources for suicide and self-harm support which are continually iterated, with the support of experts.

**2. Age-appropriate application**

Yes

☐ Age verification:

☐ First, we would like to emphasise that no age verification mechanism can achieve 100% accuracy; there will always be ways to circumvent even the most robust measures.

☐ For our part, Facebook undertakes a series of steps to (1) prevent users under 13 from signing up for Facebook services and (2) detect underage users.

☐ When users sign up to our services, they are required to enter their date of birth. If the user enters a date of birth indicating they are under the age of 13, we do not allow them to sign up. To prevent them from being able to return and enter a different age, we place cookies on their browser so we know that we've previously blocked that browser due to an ineligible age.

☐ If a user enters a birthdate below 13, they will see a general error message so they won't necessarily know they were blocked due to entering an age lower than 13. This message also directs users to our community support team. These measures are intended to prevent or deter underage users from circumventing our policy and system.

☐ We ask people to report underage accounts and have a specific form accessible to both users and non-users of Facebook services. As soon as we become aware that an account is used by a child under 13, we delete that account. We may become aware via a specific report that a person is underage — for example from a parent or teacher. We also recently expanded our enforcement measures in this area, meaning that we will delete the accounts of underage users as part of our review of these accounts for other types of reported violations.

☐ When a reviewer of a reported account flags the account as someone believed to be under 13, we restrict access to the account so the person will not be able to use Facebook until they provide proof of their age. If the person is unable to or does not provide this proof, we will delete the account.

☐ We support Internet Matters and our Digital Safety Ambassadors Programme to ensure young people and parents are informed of the appropriate age to use our platform and how to report under age accounts.

☐ We are committed to finding additional ways to further minimise the number of young people who access our platforms inappropriately or who see content that is inappropriate. This new work will build on our long-established focus on tackling this issue, and we look forward to working with the ICO and other stakeholders to explore these options in more detail.

☐ We are working on changes to make it more challenging for people to give us an inaccurate age at sign up. For instance, we won't have a default age at or above the minimum required age to access our services.

☐ One of the next challenges we will tackle is improving our ability to proactively find people on our services who misstate their age. To address this, we are in very early stages of exploring ways to improve the effectiveness of Artificial Intelligence (AI) as a tool for identifying the age of users on our platform so we can ensure they receive an age-appropriate experience.

☐ Our conversations with parents, parenting groups and experts suggest many kids under 13 are using technology, and there is a need to provide a more safe and positive experience for them. We have collaborated with child development and other experts on a messaging service specifically designed for children under the age of 13, called Messenger Kids: https://messengerkids.com/. Messenger Kids provides parents more control and gives children under 13 a safer space to message and video chat. Parental controls are core to the experience — for instance, parents get to choose and approve who their child chats with and the sleep mode feature allows parents to set predetermined “off times” for the app on a child’s device. This feature is not yet available in the UK, but we hope to introduce it soon.

☐ Age ranges/age appropriate experiences:

☐ Giving children an age-appropriate online experience is very important to us. We have implemented robust privacy and safety measures to protect young people who use our services

☐ We provide educational signposting to young users, to help them understand the audience they're sharing with. We encourage them to only only accept friend requests from people they know.

☐ As announced by the Royal Foundation Commission on Cyber Bullying, we have also adapted our platform to provide direct access to support when teens face bullying online. We worked with the NSPCC to create new functions that introduce young people to Childline at the point that they report bullying or harassment to us.

☐ We limit the ability for unconnected strangers to interact with teens. For example, in Messenger we filter out messages from unconnected adults so teens will not see them.

☐ We protect their sensitive information such contact info, school or birthday appearing in search to a public audience, including unconnected adults.

☐ We create special default settings for teens. For instance, teens default to sharing with 'friends' only, and if they proactively decide to share more widely we provide them with an educational signposting.

☐ Because it's important for teens in particular, to think before they share their location, location sharing is off for them by default. When a teen turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location.

☐ Our facial recognition products are not available to anyone under 18.

☐ Advertisers are not allow to show ads minors that “promote products, services, or content that are inappropriate, illegal, or unsafe, or that exploit, mislead, or exert undue pressure on the age groups targeted.” This would include, for example, ads for alcohol.

☐ We require Page administrators to clarify the audience suitable for their page. They can also restrict access to under 18s depending on content. We ask that Page admins age-gate their pages when they promote regulated goods such as alcohol, tobacco, or products aimed at an 18+ audience.

☐ On Instagram we have created anti-bullying tools to ensure teens have a safe, positive experience. For example, we've built a new way to identify and report bullying in photos and we introduced a camera effect to help spread kindness in Stories: https://instagram-press.com/blog/2018/10/09/new-tools-to-limit-bullying-and-spread-kindness-on-instagram.

**3. Transparency**

Yes

☐ We recognise that transparency for children is a field where there is much work to be done, and considerable room for innovation:

☐ As a foundation, however, we believe that being transparent in a clear, plain and comprehensible way is important for all users. We apply this principle across our service and for our whole user base. Both adults and children benefit from the breadth of simple and clear cut information we provide.

☐ For instance, we have updated our Data Policy (Privacy Policy) in recent years to use more simple, clear language and to provide a more intuitive, layered approach to accessing the information: https://www.facebook.com/policy.php

☐ We've also created Privacy Basics, where users can learn more about sharing, selecting audiences, their visibility, relevant reporting channels etc. Privacy Basics also includes important sections about ads, security and safety: https://www.facebook.com/about/basics.

☐ We have created a dedicated “About Ads” section that includes information about how Facebook collects and uses data to provide relevant ads: https://www.facebook.com/ads/about/?entry_product=ad_preferences.

☐ In addition to our privacy notice and the sources listed above, Facebook provides in-line education messaging adjacent to the setting, which children will read every time when they change their settings.

☐ Companies, including Facebook, should strive for even greater visual clarity using icons and videos to explain complex data processing. In order to capture and hold the attention of children, it is important that information be provided in a way that is fun and attractive. Design has an essential role to play here.

☐ In recognition of the need for improved design approaches across all digital services, Facebook launched the Trust, Transparency and Control Labs (TTC Labs): https://www.ttclabs.net/. TTC Labs are an open platform for sharing and innovation. They contain insights from leading experts in academia, design, and law, and present prototype designs, template services and open-source toolkits for people-centric design.

☐ In February 2018 Facebook organised a Design Jam in London (https://www.ttclabs.net/event/London_Design_Jam) with the goal of brainstorming best practices to provide meaningful transparency for children. The challenge was to design innovative interfaces that recognise children as sophisticated digital users and enable them to have appropriate control over their data use.

☐ Facebook also provides a dedicated Youth Portal which is visually appealing to children who are allowed to use our services, with the aim of empowering and educating them: https://www.facebook.com/safety/youth?locale=en_GB. This is broader than privacy as it includes information which we consider essential for the children's safe experience including general tips, insider tricks, privacy and safety information, and everything else children need to have a great experience on Facebook. We have a similar Parents Portal as we believe parents play a key role in supporting their children's abilities to use online services (this also contains an introductory video to parents): https://www.facebook.com/safety/parents

☐ Facebook also makes use of videos when providing information to users. For instance, the first page of our Community Standards contains a video providing a clear and concise explanation of what our standards consist of, how users make reports of activity that goes against our standards, and what our technology and teams do about it: https://www.facebook.com/communitystandards/.

☐ Companies should draft language that's meaningful to children. It can be challenging to balance legal requirements to include certain types of information and legal phrasing on one hand, with language that's accessible and clear to children on the other. We will continue to devote resources to finding the right balance, and would also welcome guidance from regulators on the type of data protection vocabulary that is appropriate for children.

☐ Companies must also strive for transparency in offline contexts.

☐ Specific messaging within online services could be supplemented by wider media campaigns or information provided to schools and other youth organisations about data protection as it relates to children. This could be done by the organisation itself or in collaboration with regulators, government, NGOs or industry groups. Delivery of such messaging can be done through social media, conventional media campaigns, or as part of the school curriculum. Media which could be used to educate children on safe use of the internet include video clips, animations, flyers and posters.

**4. Detrimental use of data**

Yes

☐ At Facebook, one of the ways we keep young people safe online is through our strict advertising policies, particularly around regulated goods (alcohol, health supplements, tobacco) and other topics such as gambling, dating, subscription services. We are always looking to improve how we deal with potentially harmful advertising content, especially with respect to children, and will continue to discuss this important topic with policymakers and child development experts.

☐ In addition, when advertisers create ads in our system, the default minimum age to select is set at 18, so an advertiser would have to explicitly choose to target users between 13-17.

☐ Our Time Spent tools are another opportunity to foster conversations between parents and teens about the online habits that are right for them and to help make time spent on Instagram and Facebook intentional, positive and inspiring: https://newsroom.fb.com/news/2018/08/manage-your-time/

**5. Policies and community standards**

Yes

☐ As part of our GDPR preparations and compliance, we asked people to agree to our updated terms of service and review our data policy, which include more detail in response to questions about how our services work. We did not ask for new rights to collect, use or share users' data on Facebook, and we continued to commit that we do not sell information about users to advertisers or other partners.

☐ In addition, we have implemented robust tools available externally to enable our users report misuses of our platforms and activities that are against our policies and Community Standards. This includes:

☐ Facebook has developed robust Community Standards (https://www.facebook.com/communitystandards/) and rely on our community to report content that may violate those standards.

☐ Reporting links are available for every piece of content on Facebook, and our teams have worked hard to make the reporting process as speedy and user friendly as possible.

☐ On Facebook, for certain graphic content that has been reported to us but does not violate our Community Standards, we are also in a position to add an interstitial warning for adults, and age-gate for minors. Adults will see the warning and will have to click further to view the video. Children simply won't be shown the video in question.

☐ Our Social Reporting tool, launched in 2011, which empowers people to self-resolution and suggests to teenagers they reach out to someone they trust

☐ Page admins are required to clarify the audience suitable for their page and can restrict access to under 18s depending on content. We ask that page admins age-gate their pages when it promotes regulated goods such as alcohol, tobacco, or products aimed at an 18+ audience.

☐ As announced by the Royal Foundation Commission on Cyber Bullying, also adapted our platform to provide direct access to support when they face bullying online. Facebook has worked with the NSPCC to create new functions that signpost young people to Childline at the point that they report bullying or harassment to us. Unlike other platforms we rolled this out so that young people who report this to us are signposted.

**6. Default settings:**

Yes

☐ At Facebook we keep young people safe online through our policies, tools, help and support, partnerships and feedback, including:

☐ Stricter default privacy settings for teenagers and additional behind-the-scenes protection.

☐ We've designed many of our features to remind them of who they're sharing with and to limit interactions with strangers.

☐ Messages sent to minors from adults who are not friends (or friends of the minor's friends) are filtered out of the minor's inbox.

☐ Additionally, we take steps to remind minors that they should only accept friend requests from people they know.

☐ New minor users are automatically defaulted to share with 'friends' only and their default audience options for posts do not include "public."

☐ If a minor wants to share publicly, the first time they go to do so they must go to their settings to enable the option and we remind them about the meaning of posting publicly.

☐ The tool for controlling which posts other people can tag you in is switched on by default for children.

☐ Facial recognition feature is not made available for under 18s.

☐ Because it's particularly important for children to think before they share their location, location sharing is turned off for them by default. When a minor turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location.

☐ Page admins are required to clarify the audience suitable for their page and can restrict access to under 18s depending on content. We ask that page admins age-gate their pages when it promotes regulated goods such as alcohol, tobacco, or products aimed at an 18+ audience.

☐ Children's profiles cannot be found on search engines off Facebook because we prohibit them from being indexed.
☐ We don’t show search results based on children's specific profile data (high school, birthday/age, and hometown, or current city) to adults who are not connected to the children.

**7. Data minimisation**

No

If YES, then please provide details.

**8. Data sharing**

Yes

☐ When our users share and communicate using our products, they choose the audience for what they share. However, we appreciate that children will not always have the full maturity to choose their audience appropriately. Therefore, we have implemented a series of measures to ensure that they are able to share within our products in a safe manner:
☐ Children are automatically defaulted to share with ‘friends’ only, they must actively select to share more widely.
☐ We've designed many of our features to remind them of who they're sharing with and to limit interactions with strangers.
☐ When it comes to teenagers we also protect sensitive information such contact info, school or birthday appearing to a public audience.
☐ We take steps to remind teenagers that they should only accept friend requests from people they know.
☐ Because it's important for young people in particular to think before they share their location, location sharing is off for them by default. When either an adult or teen turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location.
☐ We set out clear information our Data Policy, in the “How is this information shared?” section: https://www.facebook.com/policy.php. We have included selected sections here:
☐ People and accounts you share and communicate with: “When you share and communicate using our Products, you choose the audience for what you share. For example, when you post on Facebook, you select the audience for the post, such as a group, all of your friends, the public, or a customized list of people. Similarly, when you use Messenger or Instagram to communicate with people or businesses, those people and businesses can see the content you send. Your network can also see actions you have taken on our Products, including engagement with ads and sponsored content. We also let other accounts see who has viewed their Facebook or Instagram Stories. Public information can be seen by anyone, on or off our Products, including if they don't have an account. This includes your Instagram username; any information you share with a public audience; information in your public profile on Facebook; and content you share on a Facebook Page, public Instagram account or any other public forum, such as Facebook Marketplace. You, other people using Facebook and Instagram, and we can provide access to or send public information to anyone on or off our Products, including in

other Facebook Company Products, in search results, or through tools and APIs. Public information can also be seen, accessed, reshared or downloaded through third-party services such as search engines, APIs, and offline media such as TV, and by apps, websites and other services that integrate with our Products."

□ Apps, websites, and third-party integrations on or using our Products: "When you choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what you post or share. For example, when you play a game with your Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about your activities in the game or receive a comment or link that you share from the website on Facebook. Also, when you download or use such third-party services, they can access your public profile on Facebook, and any information that you share with them. Apps and websites you use may receive your list of Facebook friends if you choose to share it with them. But apps and websites you use will not be able to receive any other information about your Facebook friends from you, or information about any of your Instagram followers (although your friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies, not this one. Devices and operating systems providing native versions of Facebook and Instagram (i.e. where we have not developed our own first-party apps) will have access to all information you choose to share with them, including information your friends share with you, so they can provide our core functionality to you. Note: We are in the process of restricting developers' data access even further to help prevent abuse. For example, we will remove developers' access to your Facebook and Instagram data if you haven't used their app in 3 months, and we are changing Login, so that in the next version, we will reduce the data that an app can request without app review to include only name, Instagram username and bio, profile photo and email address. Requesting any other data will require our approval."

□ Advertisers: "We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission."

□ We also set out how we respond to law enforcement requests or to prevent harm:

□ "We access, preserve and share your information with regulators, law enforcement or others:

□ In response to a legal request, if we have a good-faith belief that the law requires us to do so. We can also respond to legal requests when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.

☐ When we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. For example, if relevant, we provide information to and receive information from third-party partners about the reliability of your account to prevent fraud, abuse and other harmful activity on and off our Products.
☐ Information we receive about you (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.”

**9. Geolocation**

Yes

☐ At Facebook, we recognise the important of keeping children's location private in order for them to be safe in the real world. We have implemented the following measures in relation to geolocation:
☐ Because it's important for children in particular to think before they share their location, location sharing is off for them by default.
☐ When either an adult or teen turns on location sharing, we include a persistent indicator as a reminder that they're sharing their location.

**10. Parental controls**

Yes

o Facebook does not provide parental control mechanisms. However, we have developed dedicated, expert informed resources through the Parents Portal (https://www.facebook.com/safety/bullying/parents) in the Safety Center (https://www.facebook.com/safety). This helps parents and caregivers to learn some of the basics about Facebook, get tips on how to start a conversation about online safety with their children and access external expert resources. It is mobile friendly, includes step-by-step videos and available in over 60 languages:
https://www.facebook.com/safety/parents.
o Our Time Spent tools are another opportunity to foster conversations between parents and teens about the online habits that are right for them and to help make time spent on Instagram and Facebook intentional, positive and inspiring: https://newsroom.fb.com/news/2018/08/manage-your-time/

**11. Profiling**

No

If YES, then please provide details.

**12. Nudge techniques**

Yes

☐ As we've exemplified previously, we have put in place a series of measures in Facebook to ensure that children who are allowed to use our services do so in a protected manner. In other words, we endeavor to use “positive” privacy nudges, in particular for children:

☐ We've designed many of our features to remind young users of who they're sharing with and to limit interactions with strangers.

☐ We take steps to remind children that they should only accept friend requests from people they know.

☐ Because it's important for children in particular to think before they share their location, location sharing is off for them by default. When either an adult or children turn on location sharing, we include a consistent indicator as a reminder that they're sharing their location.

☐ Our Time Spent tools are another opportunity to foster conversations between parents and teens about the online habits that are right for them and to help make time spent on Instagram and Facebook intentional, positive and inspiring: https://newsroom.fb.com/news/2018/08/manage-your-time/

☐ On Instagram, we are currently testing making “like” counts invisible in feed – people will still be able to actively engage with a post by liking it, but by hiding numbers we hope people will focus on the photos and videos being shared, not how many likes they get. See an example of recent press reports here: https://techcrunch.com/2019/04/18/instagram-no-like-counter/

**13. Connected toys and devices**

No

If YES, then please provide details.

**14. Online tools**

Yes

☐ We provide a dedicated section in our Data Policy for people to learn about how to exercise their rights under the GDPR: https://www.facebook.com/policy.php. In addition, we provide a variety of tools for users, including children, to exercise their rights.

☐ In preparation for the GDPR, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. Instead of having settings spread across nearly 20 different screens, they’re now accessible from a single place. We’ve also cleaned up outdated settings so it’s clear what information can and can’t be shared with apps.

☐ People have also told us that information about privacy, security, and ads should be much easier to find. The new Privacy Shortcuts is a menu where you can control your data in just a few taps, with clearer explanations of how our controls work. For more information, please see here: https://newsroom.fb.com/news/2018/03/privacy-shortcuts/.

☐ Right to access:

☐ Through the Access Your Information tool, we have made it straightforward for all people on Facebook to access their information and information about them.

☐ We also offer an email alias (datarequests@support.facebook.com) that minors can use to contact our specialist team directly to submit their access request.

☐ Right to portability:

☐ Through the Download Your Information tool, we have made it easy for all people on Facebook to download their information, either for their own use or to take to another service.

☐ Right to object and right to restrict processing:

☐ We provide a form for people to exercise their rights to object and restrict processing: https://www.facebook.com/help/contact/367438723733209.

☐ Right to erasure:

☐ In the context of Facebook's services where children are 13 or older, and consistent with Article 16 of the UN Convention on the Rights of the Child, a child is able to make an erasure request by herself or himself.

☐ We have made it easy for users to delete the personal content they have posted historically as they continue to grow and evolve as individuals. As part of our GDPR preparations, we also improved our Settings tab so users can more easily view and edit or delete the content they've posted.

☐ Where parents believe Facebook content should be deleted, particularly where this relates to photos and videos which violate Facebook's Community Standards, they can report content that has been posted by someone else and have it erased if their child in the photo or video is under 13 by filling out this form (https://www.facebook.com/help/contact/144059062408922)Where the child is over 13, we encourage the parent and child to work together to submit a request using this form (https://www.facebook.com/help/contact/144059062408922). Photos or videos involving anyone else (other than the child) will need to be reported by the relevant individual. We also take into consideration when a reported photo or video involves potential violations of a minor's privacy and, on balance, are more likely to remove in these circumstances where a minor is involved.

☐ Generally, we do not close or disable accounts of users between 13 and 18 because a parent has requested it.

☐ Parents or family members may ask us to remove an account if the person is physically or mentally incapacitated. We also work with safety partners who may be able to frame sensitive family situations and for us to provide support to a family in distress.

☐ In any event, all Facebook users can delete information they've uploaded or shared on Facebook at any time in their Activity Log on a per item basis, and the design of our platform makes it easy for users to do so

**15. Data protection impact assessments**

No

If YES, then please provide details.

**16. Governance and accountability**

Yes

☐ GDPR fundamentally changed the way Facebook works. We have updated our privacy policies and implemented a series of internal measures to ensure that there is ongoing compliance and accountability:

☐ We've expanded our Data Protection team in the EU and we'll keep growing.

☐ Our privacy operations team works around the clock to make sure we're addressing people's questions about their data.

☐ The Office of our Data Protection Officer was established in May 2018 and is working to fulfill its statutory obligations under the GDPR to monitor and advise on Facebook's compliance with the GDPR, including provisions related to the processing of children's data.

☐ Besides having internal policies and procedures in place as well as teams dedicated to privacy and data protection, we provide training on data protection as well as information security to all of our staff including employees, contingent workers and interns.

**Q5.** Do you think this standard gives rise to any unwarranted or unintended consequences?

1. **Best interests of the child**

No

As stated above, we would encourage the ICO to work with industry, child development experts, and others to create a more detailed balancing test to weigh the various interests of the child and avoid unintended consequences.

**2. Age-appropriate application**

Yes

☐ On age ranges:

☐ It is clear that young people need special attention when it comes to their privacy and safety online. The age ranges in the proposed code could potentially restrict services to children of similar developmental capacities, and we suggest that brackets should be broad enough to allow design differences that are not artificial. Narrowness of age groups could be problematic for young people who require access to support systems or other information online to help them learn and express their views.

□ It is also worth noting that age is an imperfect measure of maturity. Parents are in the best position to evaluate if their children are ready for certain online experiemces. Therefore, the ICO's guidance should be flexible enough to empower parents to make decisions with their children about what is appropriate in their particular circumstance.

□ On age verification mechanisms:

□ Technology, communication, and social interaction are not inherently harmful, and it is important to ensure that both children and adults maintain access to services, support systems and other information online that allow them to express their views, exercise their right to free expression, and connect with meaningful communities, hobbies, interests, and learning.

□ Interfaces should thoughtfully reflect the needs of the person using the service, their level of knowledge and should be appropriate to the use case. This means suitably reflecting the context, as opposed to simplifying controls for young people who are often highly capable in using digital services.

□ Measures to check age should be proportionate to the risks posed to children, without creating unnecessary friction to accessing digital services, learning, and becoming empowered. There are millions of people online who often don't have means to prove their age or identity (e.g., if they don't have an ID or other official document). While there may be a role for AI/machine learning to play, these technologies are still under development.

□ It's also important to keep in mind that different services create different expectations and risks/benefits. For instance, a service that collects and processes minimal personal data, such as an encrypted messaging service, will want to minimize any further data collection and retention, including pushing back on any requirement to obtain ID documents.

□ As exemplified above, Facebook already employs a number of methods to ensure users are the appropriate age, and we are committed to finding additional technology-driven solutions to further minimise the number of young people who access our platforms inappropriately or who see content that is inappropriate.

**3. Transparency**

Yes

□ As companies develop and enhance their communication to children, they must find solutions to a number of challenges:

□ Young people understand and access digital services differently than adults; they may have different expectations and favour different designs.

☐ Children do not represent a homogeneous demographic group. Even within similar age categories, children may have differing capacities to understand information depending on their literacy level, cultural background, and education.

☐ There is tension between providing the level of detail required by the GDPR (e.g. Articles 13 and 14) and informing different age groups in a simple and comprehensible manner. Over-simplifying the language might create the risk of underplaying or obscuring the companies' compliance with the GDPR.

☐ When companies provide information to both adults and children, they must decide whether to create different versions of a document — one for children and one for adults. Unfortunately, creating two different versions as well as complementary 'bite-sized' information could risk legal uncertainty as to the exact interpretation of the terms used and about the information being transmitted. The majority of companies have created only one version of their terms of service or privacy policies/notices, rather than a separate version for children.

☐ The ICO's position is not sufficiently clear as to what level of information provided by organisations to children and parents will be considered for compliance with (i) Articles 13 and 14 (i.e., will consist of the 'privacy notice') and (ii) the principle of transparency set out in Article 5(a) of the GDPR. In other words, we invite the ICO to clarify whether the 'bite-sized' information, or any other additional information provided beyond the privacy notices, will be considered to form part of these notices. This additional information would naturally be written in different language, with simpler terms used for transparency purposes, in particular if directed to children. Therefore, if considered part of the privacy notice there could be a risk of conflict of interpretation and therefore noncompliance with Articles 13 and 14.

☐ To date, Facebook has provided information to all users via our Data Policy in a unified manner in order to avoid confusion and ensure consistency. We are looking forward to continued dialogue on how to provide appropriate information to different age groups, including adults and children, in a way that is meaningful and does not put organisations or users at risk of uncertainty.

**4. Detrimental use of data**

No

If YES, then please provide your reasons for this view.

**5. Policies and community standards**

No

If YES, then please provide your reasons for this view.

**6. Default settings**

No

If YES, then please provide your reasons for this view.

**7. Data minimisation**

Yes

□ The Code advises that “You should avoid collecting real world identifiers whenever possible, making use of options such as avatars and user names instead.” However, Facebook is a service where everyone uses the name they go by in everyday life. For our users, knowing who they're connecting with helps keep them and the rest of the community safe from impersonation, scams, phishing, and other potential harms. We advise the ICO to clarify that “real world identifiers” would not encompass policies like Facebook's authentic name policy.

□ We would also encourage the ICO to examine the proposed requirements of this section in relation to the age verification requirements in Standard #2. Verifying a data subject's age could lead to collecting more information than needed for the provision of the services, and also from many people outside of the relevant age bucket of 13-18, which would go against the GDPR principle of data minimisation. Traditional age verification methods involve, for instance, requesting documents from individuals in order to verify their identity (e.g. ID, birth certificate and passport), as well as other information such as credit card numbers and telephone numbers. In the case of many online services, this type of information would not be originally required for the provision of the service.

**8. Data sharing**

No

If YES, then please provide your reasons for this view.

**9. Geolocation**

No

If YES, then please provide your reasons for this view.

**10. Parental controls**

No

If YES, then please provide your reasons for this view.

**11. Profiling**

Yes

Please see our response to Question #4.

**12. Nudge techniques**

No

If YES, then please provide your reasons for this view.

**13. Connected toys and devices**

No

If YES, then please provide your reasons for this view.

| |
|---|
| **14. Online tools** |
| No<br><br>If YES, then please provide your reasons for this view. |
| **15. Data protection impact assessments** |
| No<br><br>If YES, then please provide your reasons for this view. |
| **16. Governance and accountability** |
| No<br><br>If YES, then please provide your reasons for this view. |

**Q6.** Do you envisage any feasibility challenges to online services delivering this standard?

| |
|---|
| 1. **Best interests of the child** |
| Yes<br><br>Without a more detailed balancing test that could be operationalised, it should be noted that each company may employ different approaches to determining the best interests of the child. |
| **2. Age-appropriate application** |
| Yes<br><br>☐ On age ranges:<br>☐ It is clear that young people need special attention when it comes to their privacy and safety online. The age ranges in the proposed code could potentially restrict services to children of similar developmental capacities, and we suggest that brackets should be broad enough to allow design differences that are not artificial. Narrowness of age groups could be problematic for young people who require access to support systems or other information online to help them learn and express their views.<br>☐ It is also worth noting that age is an imperfect measure of maturity. Parents are in the best position to evaluate if their children are ready for certain online experiemces. Therefore, the ICO's guidance should be flexible enough to empower parents to make decisions with their children about what is appropriate in their particular circumstance.<br>☐ On age verification mechanisms:<br>☐ Technology, communication, and social interaction are not inherently harmful, and it is important to ensure that both children and adults maintain access to services, support systems and other information online that allow them to express their views, exercise their |

right to free expression, and connect with meaningful communities, hobbies, interests, and learning.

☐ Interfaces should thoughtfully reflect the needs of the person using the service, their level of knowledge and should be appropriate to the use case. This means suitably reflecting the context, as opposed to simplifying controls for young people who are often highly capable in using digital services.

☐ Measures to check age should be proportionate to the risks posed to children, without creating unnecessary friction to accessing digital services, learning, and becoming empowered. There are millions of people online who often don't have means to prove their age or identity (e.g., if they don't have an ID or other official document). While there may be a role for AI/machine learning to play, these technologies are still under development.

☐ It's also important to keep in mind that different services create different expectations and risks/benefits. For instance, a service that collects and processes minimal personal data, such as an encrypted messaging service, will want to minimize any further data collection and retention, including pushing back on any requirement to obtain ID documents.

☐ As exemplified above, Facebook already employs a number of methods to ensure users are the appropriate age, and we are committed to finding additional technology-driven solutions to further minimise the number of young people who access our platforms inappropriately or who see content that is inappropriate.

**3. Transparency**

Yes

We believe that further multi-stakeholder discussion is needed with regards to finding a balance between providing different levels of information to children and still having certainty that this would be compliant from a legal and regulatory perspectives. We would welcome the opportunity to continue exploring this issue with the ICO and experts in UX/UI design for children.

**4. Detrimental use of data**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**5. Policies and community standards**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**6. Default settings**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**7. Data minimisation**

Yes

☐ The Code advises that "You should avoid collecting real world identifiers whenever possible, making use of options such as avatars and user names instead." However, Facebook is a service where everyone uses the name they go by in everyday life. For our users, knowing who they're connecting with helps keep them and the rest of the community safe from impersonation, scams, phishing, and other potential harms. We advise the ICO to clarify that "real world identifiers" would not encompass policies like Facebook's authentic name policy.

☐ We would also encourage the ICO to examine the proposed requirements of this section in relation to the age verification requirements in Standard #2. Verifying a data subject's age could lead to collecting more information than needed for the provision of the services, and also from many people outside of the relevant age bucket of 13-18, which would go against the GDPR principle of data minimisation. Traditional age verification methods involve, for instance, requesting documents from individuals in order to verify their identity (e.g. ID, birth certificate and passport), as well as other information such as credit card numbers and telephone numbers. In the case of many online services, this type of information would not be originally required for the provision of the service.

**8. Data sharing**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**9. Geolocation**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**10. Parental controls**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**11. Profiling**

Yes

☐ The ICO recommends that ISS should “ensure features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise)”. Examples of compelling reasons include child protection and safeguarding.

☐ Following this recommendation is not possible when the core service provided consists of personalisation.

☐ There are other ways that ISS can protect children when they provide personalisation of content as a service.

☐ Content:

☐ At Facebook we require Page admins to clarify the audience suitable for their page, and they can also restrict access to under 18s depending on content. We ask that Page admins age-gate their pages when it promotes regulated goods such as alcohol, tobacco, or products aimed at an 18+ audience.

☐ We also encourage our users to share responsibly as part of our terms and conditions. But responsible sharing doesn’t always mean content is suitable for our younger users. In early 2015, we began to age gate content that comes to our attention that is not appropriate for children but doesn’t actually violate our policies. So, for certain graphic content, e.g. animal cruelty (posted in condemnation or to raise awareness), or a video of someone being shot, adults will see the warning screen and can decide to view the content, but children simply don’t see the content in question - it is age-gated.

☐ Newsfeed and Advertising controls:

☐ We've long had controls for users so they can play a role in ensuring their personalised Facebook is right for them. Recently we announced updates to our Newsfeed and Advertising transparency and controls, called “Why am I seeing this?”: https://newsroom.fb.com/news/2019/03/why-am-i-seeing-this/. These updates help users better understand and more easily control what they see from friends, Pages and Groups in your News Feed. This is the first time that we’ve built information on how ranking works directly into the app.

☐ We provide additional information about how people can control their personalised advertising experience on Facebook on our About Ads page: https://www.facebook.com/about/ads

**12. Nudge techniques**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**13. Connected toys and devices**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**14. Online tools**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**15. Data protection impact assessments**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**16. Governance and accountability**

No

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

**Q7.** Do you think this standard requires a transition period of any longer than 3 months after the code come into force?

1. **Best interests of the child**

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

**2. Age-appropriate application**

Yes

☐ If standards are to be used as the basis for enforcement by an authority, they should be sufficiently clear and specific to enable companies to comply. Where a standard can only be reached with technical means that are not yet available, or not yet available in a form that would allow their use in a scalable way, then this should be taken into account.

☐ We encourage further multi-stakeholder discussion concerning how to best apply age ranges and what would be the mechanisms to ensure that children use online services that are appropriate to their age. Once best practices are established, the new design, development, user testing, and a launch will require several months of work for multiple teams in a company. We suggest a transition period of at least one year after the Code comes into force.

**3. Transparency**

Yes

We believe that further multi-stakeholder discussion is needed with regards to finding a balance between providing different levels of information to children and still having certainty that this would be compliant from a legal and regulatory perspectives. We would welcome the opportunity to continue exploring this issue with the ICO and experts in UX/UI design for children.

**4. Detrimental use of data**

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

**5. Policies and community standards**

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

**6. Default settings**

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

**7. Data minimisation**

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

**8. Data sharing**

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

**9. Geolocation**

No

|  |
|---|
| If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why. |
| **10. Parental controls** |
| No<br>If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why. |
| **11. Profiling** |
| No<br>If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why. |
| **12. Nudge techniques** |
| No<br>If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why. |
| **13. Connected toys and devices** |
| No<br>If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why. |
| **14. Online tools** |
| No<br>If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why. |
| **15. Data protection impact assessments** |
| No<br>If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why. |
| **16. Governance and accountability** |
| No |

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

**Q8.** Do you know of any online resources that you think could be usefully linked to from this section of the code?

1. **Best interests of the child**

No

If YES, then please provide details (including links).

**2. Age-appropriate application**

No

If YES, then please provide details (including links).

**3. Transparency**

No

If YES, then please provide details (including links).

**4. Detrimental use of data**

No

If YES, then please provide details (including links).

**5. Policies and community standards**

No

If YES, then please provide details (including links).

**6. Default settings**

No

If YES, then please provide details (including links).

**7. Data minimisation**

No

If YES, then please provide details (including links).

**8. Data sharing**

No

If YES, then please provide details (including links).

**9. Geolocation**

No

If YES, then please provide details (including links).

|  |
|---|
| **10. Parental controls** |
| No<br><br>If YES, then please provide details (including links). |
| **11. Profiling** |
| No<br><br>If YES, then please provide details (including links). |
| **12. Nudge techniques** |
| No<br><br>If YES, then please provide details (including links). |
| **13. Connected toys and devices** |
| No<br><br>If YES, then please provide details (including links). |
| **14. Online tools** |
| No<br><br>If YES, then please provide details (including links). |
| **15. Data protection impact assessments** |
| No<br><br>If YES, then please provide details (including links). |
| **16. Governance and accountability** |
| No<br><br>If YES, then please provide details (including links). |

|  |
|---|
| **Q9.** Is the '**Enforcement of this code'** section clearly communicated?<br><br>Yes<br>If NO, then please provide your reasons for this view. |

**Q10.** Is the ‘**Glossary’** section of the code clearly communicated?

Yes

If NO, then please provide your reasons for this view.

**Q11.** Are there any key terms missing from the ‘**Glossary’** section?

No

If YES, then please provide your reasons for this view.

**Q12.** Is the ‘**Annex A: Age and developmental stages’** section of the code clearly communicated?

Yes

If NO, then please provide your reasons for this view.

**Q13.** Is there any information you think needs to be changed in the **‘Annex A: Age and developmental stages**’ section of the code?

Yes

Please see our responses regarding Standard #2.

**Q14.** Do you know of any online resources that you think could be usefully linked to from **the ‘Annex A: Age and developmental stages**’ section of the code?

No

If YES, then please provide details (including links).

**Q15.** Is the **‘Annex B: Lawful basis for processing’** section of the code clearly communicated?

Yes

If NO, then please provide your reasons for this view.

**Q16.** Is this **‘Annex C: Data Protection Impact Assessments’** section of the code clearly communicated?

Yes

If NO, then please provide your reasons for this view.

**Q17.** Do you think any issues raised by the code would benefit from further (post publication) work, research or innovation?

Yes

We would value the opportunity to have further discussions with the ICO to determine how companies can work together with designers and the ICO to develop practical solutions to a number of issues raised by the code, in particular age verification, profiling, transparency and nudge techniques.

# Section 2: About you

**Are you:**

| | |
|---|---|
| A body representing the views or interests of children?<br>Please specify: | □ |
| A body representing the views or interests of parents?<br>Please specify: | □ |
| A child development expert?<br>Please specify: | □ |
| An Academic?<br>Please specify: | □ |
| An individual acting in another professional capacity?<br>Please specify: | □ |
| A provider of an ISS likely to be accessed by children?<br>Please specify: | ☒ |
| A trade association representing ISS providers?<br>Please specify: | □ |

| | |
|---|---|
| An individual acting in a private capacity (e.g. someone providing their views as a member of the public of the public or a parent)? | □ |
| An ICO employee? | □ |
| Other?<br>Please specify: | □ |

**Thank you for responding to this consultation.**

**We value your input.**