Data Protection Commission’s public consultation on the draft Fundamentals for a Child-Oriented Approach to Data Processing

1. Executive Summary

Google fully supports the Data Protection Commissioner (“**DPC**”)’s objective of protecting children. We value the extensive research conducted in formulating the draft Fundamentals for a Child-Oriented Approach to Data Processing (the “**Fundamentals**”) and welcome the opportunity to provide comments.

In this response, our overall objective is to provide practical feedback as regards ensuring that the final Fundamentals are as effective as possible in appropriately protecting children’s data protection rights, while still allowing them to have a positive experience of online services. Our comments are also intended to ensure that any unintended consequences are avoided to the greatest extent possible.

In particular, we focus on: (i) Google’s commitment to better protection for children, including concrete examples of our work on innovative products, clear policies, privacy standards and educational programmes; (ii) our comments to the Fundamentals, including uses of personalisation that can be in the best interest of the child and how the implementation of safeguards could allow for an enjoyable and safer experience for children; and (iii) our support for industry proposals which seek to enhance protections for children and enable them to have a positive experience of online services.

2. Google’s commitment to better protection for children

As technology continually develops, and potential threats to users of online services evolve on an ongoing basis, we remain committed to helping improve online safety. We are constantly working to understand the problems our users are facing through research, and developing strategies to help protect our users with updates to our products.

At Google, we believe that technology can be a force for good - unlocking creativity, fostering expression and learning skills that help children and young people build their futures. Our approach to ensure children have a fun and supportive experience while using our services is a holistic one that takes into account data protection imperatives as well as other considerations beyond this remit: security, content safety, the encouragement of good online habits and the setting of family ground rules, as well as the fostering of children’s access to knowledge, education, and the development of their autonomy. Our approach includes:

- **Building innovative products** - to be used by children and their families to help provide them with more contained, age-appropriate experiences and protections and help families develop the balance that works for them.

- **Implementing clear content policies** - we have in place extensive policies that help respond to new and evolving trends, developing industry-leading tools that help us detect abusive content at scale.
- **Protecting children's privacy -** by creating strong privacy standards for all users, and specific policies for children.
- **Educational programmes -** working with experts, including children and families, we have developed global educational programmes that help children build digital literacy and digital citizenship to better navigate life online.

2.1. Building innovative products with kids and families in mind

We develop products specifically for kids and families, fitting with their needs to enable kids to enjoy their experiences online while helping them be safer.   Examples include:

- Family Link. A downloadable app, now available by default in the latest Android operating system and Chromebooks, that helps parents stay in the loop as their child explores the internet on a compatible device. The app lets parents set digital ground rules for their family, such as managing the apps their child can use, keeping an eye on screen time, or setting a bedtime and daily limits for their child's device.
- YouTube Kids. An app that provides a separate YouTube experience designed especially for children, that parents can supervise. The app uses a mix of filters, user feedback and content moderation to keep the videos in YouTube Kids family-friendly, allowing children to explore a catalogue of content in a safer environment. YouTube Kids offers a set of parental controls to customise their child's experience. Parents can decide what content to make available for their child to watch, set a timer to control screen time, block videos or channels, and more.
- YouTube supervised experience. As of March 2021, parents using Family Link can also supervise access to YouTube, with three content settings for parents to choose from. The YouTube supervised experience will look much like YouTube's flagship app and website, but with adjustments to the features children can use and ads protections. For example, comments and live chat will be disabled, as well as the ability to upload content and make purchases. Additionally, automatic reminders will appear for breaks and bedtime, which they can adjust to reinforce healthy screen time habits.
- Expert Approved Apps. Google Play Expert Approved apps make it easier for parents to find apps that are both enriching and engaging for their children. These apps are reviewed and rated by child development experts to highlight content that helps children develop, grow and have fun.
- Google Kids Space. A tablet experience available on certain Android tablets which features high-quality apps, books and videos for children up to the age of 9. Google Kids Space invites children to Play, Make, Watch and Read by recommending certain content from the Expert Approved apps program, YouTube Kids, and Google Play Books. Children are given recommendations based on their age and selected interests.

2.2. Policies to help protect children from inappropriate or harmful content

In addition to building products to create experiences for children that are safer and more contained, we also set relevant policies. YouTube Community Guidelines set out clear categories of content that is excluded from the platform. These extensive policies include prohibitions on content that portrays graphic violence, pornographic material and hate and harassment. We have developed classifiers that help us identify and remove content from our platform at speed. We have specific child safety policies that prohibit content that may put children at risk, including content that sexualizes minors or portrays minors in situations that put them at significant physical risk. In Q4 2020, we removed 3.8m videos on child safety grounds, the majority of which were removed before they had received 10 views.[1]

In addition, we make extensive efforts to detect and remove child sexual abuse material (CSAM). We deter and detect offenses on Google products, and have invested heavily in fighting against child exploitation online. More information on the technology that we develop and share to combat CSAM and how we collaborate with others in the sector can be found here. For more information on how Google protects children from abuse, see here.

2.3. Protecting children's privacy

We understand and share parents' and educators' concerns about protecting the privacy of children.

We put in place strong privacy protections for all users, and have additional stringent requirements for children. For example, we do not serve personalised ads to users that declare to be below the age of 16 in the European Economic Area, regardless of the age of consent established by the specific country.

In addition, we have developed privacy notices for all users that are accessible and easy to understand, and that provide users with illustrations, animated videos and explanations to emphasise key aspects, such us:

- What information we collect
- Why we collect that information; and
- How to control the privacy settings.

We are also committed to transparency on our platform, and are working to provide resources that are more specifically tailored to users under the age of 18, in addition to those we have already implemented (e.g., our Disclosure for Children on Family Link).

2.4. Educational programmes

We develop educational resources that create opportunities to learn and to encourage safer and more responsible interactions online.

Our flagship educational program is Be Internet Legends —designed by experts to empower children to use the web more safely and wisely. The programme includes 'Interland', an online game that teaches the key lessons of Internet safety through games, and a resource pack for teachers that includes lesson plans and activities, as well as useful tips for parents.

In Ireland, we partner with Barnardos to offer Be Internet Legends online safety workshops to students aged 8–12, teachers and parents in schools nationwide. Since the launch in September 2019, this partnership has trained a total of 14,000 primary students, 750 parents and 220 teachers, and we hope to reach up to 900 schools over the coming years. This ambitious preventative programme is child-centred and aims to empower children to make good choices online, as well as help facilitate further conversations about online safety at home.

[1] https://transparencyreport.google.com/youtube-policy/removals?hl=en

3. The Fundamentals

As outlined above, Google fully supports the overall objective of the Fundamentals to help keep children safe online, and to help ensure a child-oriented approach to the processing of their data. We believe that an approach focused on empowering young users and their parents with educational content, transparency and privacy tools to experience the online world in a safer and concerted manner would be an effective way of meeting this objective.

In particular, consistent with Fundamental 14 ('*Bake it in*'), Google prioritises —by design and by default— having a consistently high level of data protection which is embedded across all of our services. Furthermore, as regards Fundamental 10 ('*Don't shut out child users or downgrade their experience*'), Google strongly agrees that children deserve a rich service experience and that compliance with the Fundamentals should not lead to an inferior level of central services and features offered to children. We would be concerned that offering children services of inferior quality could result in children wanting to migrate to adult services, and could be an incentive for children to bypass the protections offered to them. The result of this would be to make their experiences less safe.

3.1. Fundamental 12 (Profiling)

Google notes that Fundamental 12 ('*Profiling*') could be read as to create an almost complete prohibition on processing children's personal data for the purpose of providing them with personalised content or carrying out any other automated decision-making in relation to children, irrespective of the privacy settings that may be in place.

We also note that the proposed wording does provide for an exception where organisations can clearly demonstrate how and why profiling is in the *'best interests of the child'*. While we appreciate the DPC's objective of maximising the safeguarding of children's data protection rights, the specific determination of what is in the best interests of a child relates to child welfare issues writ large, which includes child data protection as well as other considerations, and the complexity of this determination and of the interplay between different rights may result in unintended consequences.

Drawing from our approach to, and experience of, online safety for children and processing of children's data described above, we set out as follows some comments on the potential unintended consequences of Fundamental 12 as well as some uses of personalisation that we consider can be in the best interest of the child.

<u>Role of personalisation in safeguarding children</u>

- Offering personalised content or recommendations (auto-suggestions) to children can contribute to a safer experience online. A child is more likely to be served content that is suitable to their age than if they were to proactively look for content themselves. Without a measure of personalisation, there is a potential incremental safety risk of surfacing content that is inappropriate for the specific user. For example, Google Kids Space provides for a personalised experience where the content is tailored to the child's selected interests. This allows us to provide a contained and safer place for the child while at the same time providing a rich service that they enjoy and seek to engage with rather than circumvent.

- Personalisation also allows Google to apply special safety features —such as smart filters or site blockers[2]— into many of our products to make them safer and more enjoyable for children. Parents can check content ratings to understand an app's maturity and set filters based on those ratings to decide what's right for their child.

- Certain mechanisms for age verification could also be considered a form of profiling and are needed to ensure that an appropriate experience is offered.

Removing personalisation from the services provided to children could inadvertently deprive organisations of some of the tools that are used to help protect and safeguard children, as well as some of the mechanisms that can help comply with the Fundamentals. We would ask for an interpretation of the best interest of the child in light of these potential unintended consequences.

<u>Role of personalisation in enhancing child user experience</u>

We note and welcome Fundamental 10 which, consistent with the protection of children's rights more generally, requires that organisations do not downgrade the user experience when implementing measures to minimise risks posed to children.

- Content personalisation enhances and helps provide a richer user experience for children. Many products and services depend on personalisation in order to offer the functionality expected by users. For example, in a Help Centre, information about a user's account can be used in order to ensure that the help content that is surfaced is relevant to the devices that the user owns or is most relevant to the service they were utilising last.

- It can also play a role in ensuring a fun, engaging experience, which can encourage the development of a child's interests and curiosity. For example, if a child using Google Kids Space is interested in marine life and reads a series of books on sea-life, they may receive recommendations for an app that can be used by the child to help identify marine life in the wild, which helps them take their interests offline and further explore the field of marine biology, rather than seeing a listing of irrelevant but popular apps. It is also important to note that these personalised recommendations are always mixed with other content to ensure users see a variety of content.

- Even if no profiling takes place, children will still be served suggested content, but that content will be less relevant, and based on what is generally popular on the platform. To illustrate with an example, imagine an Irish 15-year old who is studying art for their Junior Certificate, focusing on painting. Personalisation allows us to surface content about painting based on their previous interests, rather than irrelevant content that is simply popular on the platform - like music videos.

- Personalisation can help children make the most of screen time and reduce it when combined with digital wellbeing tools and parental controls when appropriate. For example, a child is more likely to be satisfied with 30 minutes of screen time if they spent 30 minutes interacting with relevant content or search results, rather than having to spend their time fine-tuning search terms to identify content that is relevant for them.

[2] https://safety.google/families/family-friendly-experiences/

Removing personalisation from the services provided to children would lead to the provision of a two-tier service, with an inferior level of central services and features offered to child users and a superior service offered to adult users. This may incentivise children to lie about their age and otherwise try to circumvent the protections set up for them in order to access services that they actually enjoy.

We think that offering personalisation to both ensure safety, and a richer user experience that is not downgraded and the child can enjoy, can be in the best interest of children when appropriate safeguards are implemented. These can include ensuring that only appropriate recommendations are offered, that meaningful controls are in place, and that wellbeing tools are offered (e.g., reminders about the time spent online). We would ask that broader uses of personalisation for the purpose of providing a rich experience are also considered in the interpretation of the processing that can be in the best interests of the child when appropriate safeguards have been implemented.

Contextualisation and other uses of data

We welcome the DPC's confirmation that contextual advertising to children which does not rely on personal data is beyond the scope of data protection law. Users benefit from contextual non-personalised ads on Google and other services every day. We would however suggest a small change in the text to reflect the fact that contextual ads use data beyond on-screen content (but not based on a profile of the user or tracking), such as operating system, device type, or IP address. We would change the wording of the Foreword to: "The issue of contextual advertising (which doesn’t rely on tracking and profiling but rather delivers advertisements based on on-screen content and other contextual signals) to children is beyond the scope of Fundamental 12 on profiling."

We similarly would change the wording of Fundamental 12 to remove or otherwise modify the reference to “or otherwise use their personal data, for marketing/advertising purposes” to clarify that the serving of contextual ads, as outlined above, and also ancillary uses of data that are necessary for ad serving, including measurement, or even spam and abuse detection and frequency capping, are not under the scope of Fundamental 12.

3.2. Children’s developmental context

The United Nations Convention on the Rights of the Child (“UNCRC”) introduced for the first time in an international human rights treaty the concept of the ‘evolving capacities’ of the child. This principle has been described as a new principle of interpretation in international law, recognising that, as children acquire enhanced competencies, there is a greater capacity to take responsibility for decisions affecting their lives. The UNCRC allows for the recognition that children in different environments and cultures, and faced with diverse life experiences, will acquire competencies at different ages. We believe that technology needs to be developed in ways that recognise the need for a balance between protecting children and allowing them to build the autonomy to take responsibility as their capacity evolves.

Extending the same treatment to all young people under 18, without any recognition of the different stages of development of children does not seem to have regard to the different abilities and needs of those children. This approach especially risks limiting the autonomy of teenagers, their access to information, and their right to express themselves, create and learn, making the best of what is available online. A blanket approach to the implementation of the requirements under the Fundamentals could effectively align the mental, developmental and emotional capacity of, for example, a 17 year old to that of a 7 year old. The consequence will be that a child, on turning 18, will be (all at once) faced with a very different online world and experience that they have never been exposed to previously and may not be equipped to navigate. Further, this generic approach risks encouraging teenagers to try to circumvent the protections set for them in order to enjoy some of the freedoms and functionalities that meet their needs and development capacity but would be restricted to them under the current proposals. This could result in an increase in the risk teenagers face without the bespoke protections that they deserve.

We acknowledge that the Fundamentals allow organisations to consider the age of a child as a factor in their approach to compliance in certain respects, for example regarding the methods used to convey transparency information and assessing the correct notification procedure in the case of data breaches. However, we would request that the Fundamentals specifically recognise the possibility to implement different approaches as necessary to appropriately protect children's privacy depending on whether the service is for young children or for an older audience.

3.3. DPC’s recommended measures for incorporating the Fundamentals

We appreciate the work of the DPC in developing guidance to interpret the Fundamentals. In this respect, we would like to highlight that, in providing guidance, technology neutral approaches that account for different types of services as well as the differences between various types of users would be encouraged.

For example, we note that the Fundamentals recommend that organisations should avoid the collection and processing of children’s biometric data. However, some products require the processing of biometric data in order to operate and, in some cases, biometric technology can be useful to protect children (including as a means of authentication or verification of age for certain situations). Additionally, processing on-device is encouraged but there are cases where it is not possible to process data on the device only.

We would also like to highlight that, whereas we are committed to continuing to evolve our technology for the protection of children, the current state of the art presents limitations that can pose challenges. Finding a balance between appropriate age verification on the one hand, and proportionality and minimisation on the other, is complex, and a granular determination of whether the user is above the age of consent can be challenging. For example, as far as we are aware, a non-intrusive mechanism for verification such as the use of machine learning to predict likelihood of the user being over 18 based on activity does not currently allow for such a granular determination. We would ask for consideration of balanced approaches that aim to determine whether the user is likely above 18, and make use of proportionate mechanisms that help achieve the objectives of the Fundamentals and address potential user concerns. In our research, we found that users are reluctant to provide a government ID and also indicated that they were uncomfortable providing their credit card details outside of the context of a payment obligation. In fact, most users felt that they would rather abandon their attempted action, than enter either a government ID or credit card as proof of their age, as they felt that they were having to place their identity and/or payment credentials at risk.

3.4. Implementation Period

As you will appreciate, the implementation of measures that strike an appropriate balance between being protective of children and guaranteeing their own rights to privacy, digital development, and autonomy in accordance with their evolving capacities, is complex and will have a significant impact on both companies and their users. Any such measures can only be introduced in a phased, gradual manner. This is necessary in order to allow for sufficient notice of the changes to be provided to users, if appropriate, or to ensure the technical changes or solutions are introduced and fully operational with minimum interruption to users and bugs.

We therefore propose that an implementation period is allowed for organisations to roll out their measures to comply with the Fundamentals.

4. **Industry codes of conduct**

We note the DPC's plans to engage with its Section 32 obligations under the 2018 Act, to encourage the drawing up of codes of conduct for various sectors that process children's data. In this regard, we are supportive of proposals which seek to enhance protections for children, and enable them to have a positive experience of online services.

As longtime members of Technology Ireland, Google strongly supported the establishment of the Online Safety Taskforce in 2019, and since then has supported the work of this Group. We believe that the protection of the interests of children can be substantially advanced through multi-stakeholder engagement, in collaboration with this Taskforce, and through codes of conduct. We look forward to working with the DPC and other important stakeholders on practical ways to implement high standards of protection for children's personal data.