DATA PROTECTION COMMISSION CONSULTATION: FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING

Observations from the Department of Education

Introduction

The Department of Education commends the office of the Data Protection Commission in its work on developing the practical implementation of data protection rights for children and notes the importance placed on the educational sector in the Fundamentals document. The Department welcomes the opportunity of sharing its views on the detailed Fundamentals document based around a balanced, rights approach to the processing of children's data. The. The observations provided are in the context of the Department of Education's mission to facilitate individuals through learning, to achieve their full potential and contribute to Ireland's social, cultural and economic development. In addition to its policy and funding role, the Department engages with schools and other educational providers through a variety of interfaces including its School Inspectorate and National Educational Psychological Services.

Any questions in relation to these observations can be directed to the Department's Data Protection Unit (DPU) by email to dpu@education.gov.ie.

General Observations

- There is repeated reference to the importance of 'clear and plain language' being used with children. However, the linguistic diversity which now exists in Ireland (foreign languages / Irish language / etc.) is not referenced in this same context. This may be worth considering as an added layer to the 'clear and plain language' discussion.

- It would be useful to produce a quick reference document which could house the key tenets of the main document and which would help with ease of access to the main points for all parties.

- The basis for the DPC's view against the setting of a general age threshold as the point at which children should be able to exercise their rights on their own behalf is well developed and understood. It would, however, be helpful to consider developing practical advice in relation to appropriate age thresholds for the exercise of rights at different levels of education in conjunction with a number of other factors of course. This is something which may be considered further in the context of developing a code of conduct.

- Transparency information needs to be understandable by children. This is a requirement that continues to be raised and discussed by the young people the Department works with. Both public and private services used by children have particular responsibility for providing clear and age appropriate information to children. The framing of terms and conditions by service providers should be done in consultation with children to help ensure children understand what

they are consenting to, in simple, plain language on different media formats. Data protection by default and design must ensure services being accessed and used by children/young people offer the highest privacy by default. Prompts should be provided if users are updating privacy settings with clear explanations provided if a user changes or updates their privacy settings. Companies could highlight what a profile setting update means for their personal information and any risks/safety concerns involved in an update. Clear guidance and expectations should be given to companies in this area.

- While noting the statement that "the Fundamentals should be complied with by all organisations processing children's data", data controllers would benefit from a clearer distinction between obligations and recommendations. Read in the context of the DPC's required compliance with the Fundamentals, is the word "recommendation" not taken as an obligation / definite requirement ?

- The age floor of protection is welcome but current age verifications are not robust. Clear guidance should be given to companies on how to demonstrate robust age verification. Guidance and clarity should be given to companies/organisation on the definition of what constitutes robust age verification.

- In general, more clarity could be given to the requirements of organisations in protecting children's data. Children need to be involved in the design process of data protection by companies, in particular social media companies.

- The issue of consent being required for the use of digital platforms for distance learning purposes in the context of the implementation of the Department of Education Circular 0074/2020 which requires schools to have a digital platform in place is important. Schools as independent data controllers add pupils/students to digital platforms and communicate with them via these means. Procedure in this regard should be included in the Acceptable Usage Policy (AUP) and this should continue to be clearly communicated to parents and children as appropriate. Schools need to list the recipients of personal data collected, particularly any commercial programmes used in their AUP, explain to children in child-friendly terms what happens to the 'data' they input on these platforms that the school will have access to. Schools need to ensure all information is clearly communicated to parents and children as appropriate including how to access their data protection rights.

- Given the large-scale move and reliance on digital platforms (platformisation) in education, it may be appropriate to include a reference to the responsibilities of the school (and all bodies engaged in education) as data controller including privacy by design and risk assessment.

- The digital world is central to children's lives and the collection and use of children's data begins at an early age continuing throughout their lifetime The Irish age of digital consent for children is 16, which means that parents must be involved in supervision up to this point. This is to ensure the protection of children particularly in online environments. It is clear that the internet poses particular challenges when it comes to children's data and there aren't necessarily clear-cut answers about what is "right" or "wrong" in every case. "Fundamentals" provision of the standards that all organisations should follow when collecting and processing children's data with its core message that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data is particularly welcome.

- Fundamental no. 9 Your Platform, your responsibility states that companies who derive revenue from providing or selling services through digital and online technologies pose particular risks to the rights and freedoms of children. Where such a company uses age verification and/ or relies on parental consent for processing, the DPC will expect it to go the extra mile in proving that its measures around age verification and verification of parental consent are effective. Children should be empowered to make informed decisions about what personal data they choose to share with an organisation or indeed with a wider audience when using an organisation's service, recommending that they seek parental/ trusted adult support or advice where they are unsure about such choices.

- If consent to process personal data is requested by the online service provider in order for the child to access the service (for example in the creation and subsequent use of a user account), parental consent must be given for that processing of the child's personal data to take place. Parents ought to be aware of the following measures from the list of examples of data protection by design and default that the DPC considers appropriate in the context of children.
    - Parental dashboard: provides parents with an overall view of activity (including any history of activity) and settings that their child has available to them.
    - Parental tracking /monitoring: Where service/ device settings allow for parents to track or monitor their child's use of online services (such as with a parental dashboard, where appropriate), transparency settings should apply so that it is visible to the child that their parent(s) can tell which app/ website/ program etc. they are using or that their parent(s) can later review their activity history.
    - Intervention: Where service/ device settings allow for parents to track or monitor their child's use of online services, consider allowing parents to modify child account controls and settings, where appropriate. Provide notifications to parents when these settings are altered, especially where location, biometrics or device sensors are involved. Ensure access to such a dashboard by parents is secured with multiple factors of authentication
    - Security: Making controls only available to parents to maintain high levels of security
    - Breaches: Notification procedures in cases of personal data breaches should account for notification to the parent rather than the child, where appropriate depending on the age of the child user affected.
    - Audience control: Where a child can share communications, content or data, ensure limited audience selections by default. Public or open sharing or even limited audience sharing may not be appropriate while sharing only with known "friends" or parents may be possible. Contact from others outside of the child's authorised contacts should be not possible for younger children 62 without parental knowledge, awareness and intervention.
    -

Observations on Specific Sections within the Document

Page	Comment
3	*About a quarter of Ireland's population are children, all of whose personal data is processed every day online and offline, in educational, health, recreational and sporting, social services, and commercial contexts.* **Comment:** Should you define children as per legislation early in the document*? In Ireland under the Child Care Act 1991, the Children Act 2001 and the United Nations*

	Convention on the Rights of the Child a child is defined as anyone under the age of 18.
3	*We are indebted to all of those schools, principals, teachers and children who generously shared their feedback.* **Comment:** It may be instructive to list children first in any collective descriptions.
4	*Beyond this consultation, the DPC is already preparing to engage fully with its Section 32 obligation under the 2018 Act to encourage the drawing up of Codes of Conduct for various sectors that process children's data. On that basis, we would be very keen to hear from stakeholders across all sectors (e.g. internet service providers, social services providers, education sector providers etc.) that would be interested in engaging with the DPC in relation to a sectoral code of conduct with the aim of driving the higher standards of protection for children's personal data required under the GDPR and creating a level playing field within sectors.* **Comment:** The Department would welcome an opportunity to be involved in any future engagement around an educational sector Code of Conduct.
4	*Jurisdictions all over the world have struggled with effective means by which age-gating could be implemented on the internet with many observers pointing out that age, in and of itself, is too blunt an instrument by which to measure capacity.* **Comment:** More than just observers – the interpretations of the UNRC and academic experts etc.
6	*This version of the Fundamentals is published for the purpose of consulting with all interested parties.* **Comment:** You may need to think of an age appropriate way to communicate the contents of this document with younger children as they are key stakeholders.
8	*The DPC notes that complying with an age-appropriate/child-oriented regime of data protection will involve costs and take creativity on the part of service designers, however, children are one in three users, and represent the adult market of the future.* **Comment:** Is age-appropriate a useful term in this context? Given that 16 years of age is the agreed age of digital consent in Ireland, there exists a huge range in what is age-appropriate for pre-schoolers, primary school-aged children and post-primary aged students….you may need to think about a minimum of what is age-appropriate at for these three stages in child development.
10	*Appendix* **Comment:** Would it be useful to add the UNCRC text to the appendixes as well?

18	*Having ratified the UNCRC in 1992, Ireland has an obligation under international law to respect, protect and fulfil the rights of children set out in the UNCRC.* **Comment:** There are also the clarifications from the UN Committee on the Rights of the Child which elucidate the Articles. Article 43(1) of the UNCRC establishes a monitoring and advisory body called the Committee on the Rights of the Child (hereafter 'Committee') as the authoritative international expert body of the UNCRC. The Committee monitors states parties' compliance through a reporting system; states parties provide general information about their country and children, and indicate measures and progress, as well as difficulties, in implementing the UNCRC. In addition, the Committee receives shadow reports on the government's implementation progress from non-governmental organisations, as well as information from other sources, including UN agencies, academic institutions and the press. Upon review of the reports and accompanying information, the Committee publishes its concerns and recommendations, referred to as concluding observations. The observations also typically offer suggestions and recommendations to the state concerned for improving compliance with the UNCRC. Analysis shows that the concluding observations increase the likelihood for changes to happen (Child Helpline International, 2014). Elsewhere, General Comments of the Committee augment the potential of the UNCRC by providing greater guidance on the obligations of states parties.
19	*The UN Committee on the Rights of the Child20 (the UN Committee) has stated that …. the following elements should be taken into account when assessing the child's best interests: The child's right to education.* **Comment:** The right to an education could be emphasised further in the context of requiring profit based online platforms to go the "extra mile" in ensuring both data protection rights and educational access are respected. For example, blocking of educational platforms should not be an expedient alternative to investment in better data protection protocols for critical educational platforms.
22	*Where practicable, an assessment of capacity in addition to age, provides a good understanding of the likely capacity at which a child may be able to comprehend a demand or situation, or an age where what is being demanded is beyond their capacity.* **Comment**: What does an assessment of capacity entail? Is this an assessment of cognitive ability? Some guidance on how 'capacity' is assessed would be helpful.
23	*In this context, there may be specific functions (legal basis performing a public task) which are required to be performed by organisations captured by this legal basis which require the processing of children's personal data e.g. in connection with health, social care or education. As a particular point of note in relation to processing carried out for such official or public tasks, the DPC's position is that organisations processing personal data under this legal basis should comply with these Fundamentals, save where the public interest*

	and/ or the best interests of the child require otherwise and the organisation can demonstrate why/ how this is the case. The Department expect that schools would benefit from references to lawful purposes other than consent for the delivery of their statutory educational services in the guidelines. On page 3 it mentions that the Irish digital age of consent will begin to be reviewed from next year so this would seem an important facet to include in that review.
26	*The GDPR requires that individuals must be given certain key pieces of information about the use of their personal data by an organisation and that this information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The clarity of this information is particularly required where it is being provided to a child.* **Comment:** The different stages of childhood are relevant too – what will suit the understanding of a fourteen year old will not suit a four year old…
26	*Recital 58: (…) Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.* **Comment:** What about children with communication difficulties- could images or pictures be used to support understanding?
27	*However, where organisations fall within the scope of application of these Fundamentals (see Section 1.3), organisations must assess how to ensure meaningful transparency for child users, according to the age ranges of child users.* **Comment:** Welcome reference to the age ranges of child users
28	*Organisations should be open and honest about exactly what it is they are doing with children's personal data indicating all of the different ways in which it will be used. This information should also be available in an obvious, easy-to-find place, e.g. not in tiny writing at the bottom of a webpage or app screen. As detailed further in Section 7, information should not appear in a way that nudges the user to accept, for example by appearing as a pop up or making the option to consent more obvious or less obstructive to the user experience than the option to find out more or withhold consent.* **Comment:** This is welcomed. *Organisations should consider using non-textual measures, such as cartoons, videos, images, icons, or gamification, depending on the age ranges of their users, to convey data protection information to children and young people more effectively, as these methods are more likely to resonate with children than blocks of text.* **Comment:** This is welcomed ('text' presented in accessible forms)
29	*The DPC considers that, in addition to data protection by design and default (see Section 7.2), organisations should actively promote privacy-protective measures amongst children by encouraging them to be curious and cautious about the use of their personal*

	data. **Comment:** This is a really good point that could be emphasised really strongly in the Professional Development Service for Teachers (PDST) *Webwise* programme for primary children.
29	**Comment:** Good to see feedback from children represented
30	*Organisations should consider using methods such as just-in-time notifications to inform children and young people about any possible risks or consequences involved in sharing their personal data at a particular moment in time, for example just before they post or share something online…..* **Comment:** This is welcomed
32	**Comment:** Good to see feedback from children represented
34	*However a child should not be considered to be competent if it is evident that he or she is acting against their own best interests.* **Comment:** While this is welcome practical advice, an example may help illuminate what is meant in practice by adding "In sum, a child may exercise their own data protection rights at any time, as long as they have the capacity to do so and it is in their best interests" and "In all events, the DPC position is that a child should be able to exercise their data protection rights, whether directly or with assistance/ representation, and should not be prevented from doing so as a result of their age, maturity or capacity." Does this mean that even if a controller denies one right (access for example), the child's other rights (information for example) should be fully respected and the child should be assisted on how to better exercise the right denied.
33	*Children of different ages have different levels of understanding and needs, and there is no "magic age" at which a new level of understanding is reached.* **Comment***:* This point is extremely valid.
38	"The purpose for which the parent(s)/ guardian(s) seek(s) to exercise the child's data protection rights – for example is this purpose wholly in the best interests of the child or is there another purpose or interest (i.e. that of the parent/ guardian or a third party, as opposed to the child) pursued in seeking to exercise these rights?;" **Comment***:* As it is not always clearly established what the purpose of a request is, advice regarding the importance of ensuring the parent / guardian who has requested the child data has sole / joint custody is important. For example, if in any doubt about whether the provision of the data is in the best interests of the children, it may be appropriate to

	clarify custody arrangements and obtain the consent of both parents/guardians in some cases.
39	*However, as regards the degree of certainty to be established by online service providers that consent has been given by the holder of parental responsibility, the GDPR requires that the online service provider must make "reasonable efforts" to verify this "taking into consideration available technology".* **Comment:** This is a welcome move as it is felt there is very little evidence of this happening in reality…
40	**Comment:** Helpful to see broad reflections from parents.
42	*"allowing access to its service – for example where an organisation provides an adult-only service which by law it cannot provide to under 18s e.g. gambling related services"* *"Compliance with the requirements of these fundamentals in no way justify the 'locking out' of children from a rich user experience' or "access to a more fulsome 'adult' service"* **Comment:** How can these competing directives be reconciled?
48	*"The soft opt-in" rule* **Comment:** Clarity or an example here in a sidebar would be helpful
48	*"Legitimate interest"* **Comment:** Further clarity on this lawful basis and its limitations in the public sphere would be helpful. Is there an assumption here of understanding?
48	*Having .. the DPC notes the concern that online age verification measures may be perceived by children as blocking them from the more complete "full" service offering, or as blocking them from accessing other features of the service they are seeking to use. compliance with the requirements of these Fundamentals, in no way justify the "locking out" of children from a rich user experience simply on the basis of purported data protection compliance.* **Comment:** There is an important risk based balance between ensuring equitable access to online educational services and ensuring the protection of the best interests of younger children through age appropriate informed consent and the oversight of parents where appropriate. While digital consent is therefore not a measure to prevent access by children to certain websites, nor should it be used as a route to treat children of all ages as if they were adults.
49	*"In this regard where the personal data of children is being processed for direct marketing purposes, whether the marketing is done through electronic forms or otherwise, (as noted above and below, this must be compliant with the requirements for legal basis and the best interests principle), it should be made clear to children that they*

	may object to the use of their data in this way." **Comment:** Made clear and accessible to children.
50	*The following list contains a non-exhaustive selection of criteria which should be taken into account in adopting a risk-based approach to verification. -type of service being offered to the child – e.g. video or image hosting platform, educational service, healthcare or social support service, social media app facilitating connections with known parties or with strangers, gaming website, shopping platform, etc.* **Comment:** The inclusion of education is welcomed in this context but the term may benefit from a clear definition in order to avoid its overly wide application.
51	*"This applies both where consent is relied on (whether given by a child, or a parent/ guardian on their behalf, as applicable) and equally where an organisation relies on one of the other applicable provisions to carry out electronic direct marketing activities, such as the "soft opt-in" rule described above which applies in the context of obtaining a person's contact details through a customer relationship."* **Comment:** This definition would be helpful earlier - see comment ref page 48
52	*In a similar vein, the EDPB has also recognised that children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising.* **Comment:** This would be particularly concerning in terms of our more vulnerable children, children with special needs, with language difficulties etc.
53	**Comment:** Children's voices here are welcomed.
54	*"organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so"* **Comment:** Also welcomed.
54	*Equally, children are less likely to be aware that these platforms are free to users because they gather and sell/ share vast amounts of their data – including automatically derived metadata such as time stamps (as to when sites or apps were visited or interactions conducted on them) and location data – to data brokers and data analytics companies who can use it to target them with personalised ads.* **Comment:** This could be a very important aspect to include in the PDST Webwise programme for senior primary school pupils to help them understand what happens with their personal data and that there is no such things as a free service.
59	*"Turn off geo-location by default for child users"*

	Comment: Strongly agree. Children accept this as a 'norm' which it is not. *"Restrict/control access to children's personal data by internal members of staff"* **Comment:** Strongly agree.
59	*"7.3 RECOMMENDED MEASURES FOR INCORPORATING DATA PROTECTION BY DESIGN AND BY DEFAULT TO PROMOTE THE BEST INTERESTS OF CHILD USERS"* **Comment**: Helpful succinct capturing of all recommendations.