Response to the ICO Consultation on a Code of Practice for Age Appropriate Design from defenddigitalme

About defenddigitalme

defenddigitalme is a non-profit, non-partisan, data privacy and digital rights group led by parents and teachers. We aim to make all children's data safe, fair, and transparent across the education sector. Our work is funded through an annual grant from the Joseph Rowntree Reform Trust Ltd.

We thank everyone who contributed to our thinking and shaping of this response including a wide range of NGOs and civil society organisations, parents, organisations representing young people, academics, developers and designers, and supporters.

September 2018

Contents

Introduction

1. The Age Appropriate Design Code of Practice starts from precepts of the GDPR, and seeks to articulate and embed better Data Protection rights for children in ISS by design, and should set out principles that can be applied across an entire device solution or ecosystem.

2. **Safeguards are missing in the UK Data Protection Act 2018 that GDPR requires in several places, such as in Clause 13 of the Act (automated decision-making authorised by law: safeguards), and 14 (exemptions) which do not address the required safeguards of GDPR 23(2) for children, at all. These should be included.**

3. The edges of definitions are unclear are many parts of the UK Data Protection Act 2018, on public interest and significant effect, and remain unclear for schools, other public bodies, and ISS providers for example, regards Right to Object. The Code could add clarity and give confidence to data processors in these regards.

4. A code should breathe life into the explicit recommendation of the Working Party 29 to create guidance on automated decision-making with significant effects and profiling in Recital 71, such a measure 'should not concern a child' and principle of Recital 38, that children "merit specific protection."

5. The Age Appropriate Design Code of Practice should however not conflate solutions for the problems of social interactions and parenting in a digital environment, with the construction of a workable Data Protection framework. ISS will follow a Code because it is statutory. Parents and children will only work within it, as long as they find its implications satisfactory, and can understand, act on, and enforce their rights under it, and in everyday terms.

6. As research[1] by Boyd, Hargittai, Schultz and Palfrey found in 2011 on US COPPA and other US children's privacy laws — such as the "Do Not Track Kids Act of 2011" (U.S. Congress, 2011) — perceived over restriction can encourage workarounds, "*it is important to understand the unintended consequences of these age–based approaches to privacy protection."*

7. *"Parents are concerned about children's safety and privacy, and governmental agencies have every reason to want to step in and help, but restricting access — or creating regulatory solutions that encourage companies to restrict access — is counterproductive. New solutions must be devised that help limit when, where, and how data are used, but the key to helping children and their parents enjoy the benefits*

[1] Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act' by Danah Boyd, Eszter Hargittai, Jason Schultz, and John Palfrey. *First Monday*, Volume 16, Number 11 - 2011 https://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075

of those solutions is to abandon age–based mechanisms that inadvertently result in limiting children's options for online access."

8. This Code should not create more friction in using ISS which is not perceived as adding any value to the user. Parents and children lie, and will continue to lie, to enable children to access services, but the Code must not mean that lying becomes the normalised workaround. Users should not be penalised for imposed protections done in their name, but rather be able to be in control of the implications of 'best interests design' themselves.

9. While a threat model is one lens through which risks to the child can be viewed, it implies a consequentialism of personal data processing, that may not be understood by a child. Rights must therefore have high standing and children's rights be respected by ISS by default.

10. When contextualizing children's right to privacy among their other rights, best interests and evolving capacities however, "i*t becomes evident that children's privacy differs both in scope and application from adults' privacy.*"[2]

11. Capacity is more appropriate than age when it comes to digital understanding and capability, especially to appropriately design for young people with disabilities, and be as inclusive as possible. Research from 2009[3] on consent and children in practice is still relevant, though we accept that it is age not capacity that is in the Act.

12. Privacy rights and child protection rights need consideration as distinct from Data Protection rights. For children, it is important that adequate weight is given to these multiple rights, and they will sometimes appear to conflict. The right to a private and supervisory adult-free space to communicate in a forum, may be viewed by some as an unsafe space for children.

13. The lifelong implications of children's data processing matters, in particular where profiling decisions are recorded, kept and used to make decisions because profiling as a child can have unforeseeable implications as an adult if used for interventions at school[4], in insurance discounts[5], potentially in screening for university[6] or future employment.

14. It is easy to think of privacy as an individual matter but not as social contract, e.g. what if friends and family (not just platforms) share photos of a child to which they cannot consent? In other words, people should be encouraged to view individuals' rights with

[2] Privacy, Protection of Personal Information and Reputation - United Nations Children's Fund (UNICEF) (2017) https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf
[3] Protecting the Virtual Child. The law and children's consent to sharing personal data, Dowty, T. and Korff, D. ARCH 2009
[4] Research by the Cambridge Institute of Criminology using pupil data for interventions with 40 schools in London http://defenddigitalme.com/wp-content/uploads/2018/04/Cambs_Crimi_NPD.pdf
[5] US State Farm Insurance Good Student discount up to 25% reduction for 'good grades' https://www.statefarm.com/insurance/auto/car-insurance-for-teens (Accessed April 2018)
[6] I was rejected from University because of my record, Inside Time, April 3 2018 https://insidetime.org/i-was-rejected-from-university-because-of-my-record-now-im-campaigning-for-fair-treatment/

respect, and recognise a collective responsibility to uphold them. Society must learn to care about “others’ privacy” and especially in the context of ISS and a child.

15. Users need and want private channels for safe or confidential communication, for example to chat about domestic violence or abuse, and for positive discussions about themes they cannot discuss elsewhere, without fear of repercussion from parents who may disagree with their lifestyle or exploration of subjects such as religion or gender.

16. Anonymity must be possible for children to maintain online. They choose to be so online so as to develop their personality and characters to the full, to explore their development of self, and to enable and control a trusted conversation on topics that they may wish those who know them could not identify with the individual.

17. A key aim of the Code should therefore be to preserve and promote autonomy, in accordance with the changing capacity of the child, to encourage the free development of young people as capable future citizens, and support their comprehension, competence, and confidence.

Key Recital 38 (GDPR) underpins the DP principles in the Code

18. *Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.*

19. *Such specific protection should, in particular, 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.*

20. *The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.*

Geographical scope and limitations

21. Scope of where the Code would apply must be clear. Without it, we run the risk that its practical application is impossible for ISS to make workable. Children can and should be able to use a VPN to shield their system location, which for example might offer them protection from tracking and targeted advertising. Children’s nationality may remain the same but their physical location change and their experience would therefore become inconsistent. Would a child in France on holiday be able to access the same ISS as they do at home, but with different standards?

22. The ICO is responsible for the regulation of data processing by UK -established controllers. The data subjects’ nationality and citizenship is irrelevant. One would assume that this Code would apply across the ICO’s geographical jurisdiction in the same way as the Data Protection Act 2018, and be applied to all personal data processing by UK based controllers.

23. Risks:

- Unclear where the Code will be enforceable in on- and off-line jurisdictions..
- Bad actors make no changes and the good actors find it creates an economic disadvantage to doing the right thing, or so cumbersome as to be unworkable
- Non-UK based controllers of ISS may offer their services to UK children without consideration of the Code.
- Technical standards are not universally understood or always globally transferable.
- If the Code is seen as unnecessary red-tape, UK based controllers of ISS may feel incentivised to withdraw their services to UK children as a result of perceived higher reputational risk to their service provision, or to move their processing establishment outside the UK.

Code of Practice suggested key proposals

24. The proposed age brackets would be not at all appropriate if prescriptive, given that capacity and not age, is the important factor in whether a user is competent to make decisions and a recognised feature of children and the existing law today, such as Fraser guidelines and Gillick competence.

25. Any Age Verification (AV) must verify the single attribute of age, not capture date-of-birth, or more personal data. Re GDPR recital 64 on Identity Verification, “A controller should not retain personal data for the sole purpose of being able to react to potential requests.”

26. We understand that the definition of an ISS in the current EU Directive is under discussion, and may change. This speaks again to why and the Code must set out expectations of behaviour and acceptable intent, rather than acceptable and unacceptable technology specifications.

27. Ranum’s Law, “You can't solve social problems with software," should be a guiding principle in the Code.

28. Anonymous personas must be possible for children to maintain online.

29. The Code should always consider and describe whether:
    a. children have the ability to opt *in* to the highest level of controls, or
    b. children and adults must opt children *out* from controls-by-default?

    Defaults that are positive to child privacy should be on by default. Those that are negative, that increase risk and potential risks to the child, off by default.

30. Technology changes, threats change less so. Therefore the Code should not proscribe or define an acceptable practice for each technology feature, but rather a higher level of expected practice in the ecosystem to mitigate a threat.

31. Transparency-by-default of the tool, (how it works, the purposes of the ISS) and the intent of the tool (why it does what it does for the purposes of the user and the ISS), of policy and any changes in it, should all be encouraged.

32. Codify the ISS intent and then know how users and regulators can check that they do, what they say they will do, or are not doing, what they say they will not.

33. In UNCRC terms of human rights, a test of 'necessary and proportionate', fundamental data processing principles, should not be seen from the ISS utility point-of-view, but from the rights of the child, and whether the data collection and processing is proportionate to potential harm, and interference with fundamental rights and freedoms.

34. For any ISS covered by the Code, Data Protection and Privacy Impact Assessments should always be mandatory in new developments, and updated with a history of edits for product enhancements.

35. Adding "friction" that seeks to force children to be conscious users may have unintended consequences that create new, or displace risks. In short: making an application easy and desirable to use, is part of security. If you purposely require application-creators to ask children **every time** "is it okay for this application to use the camera?" the children will pursue unregulated malware and snake-oil applications to make their devices nicer/easier/faster to use.

36. The burden of maintaining age appropriate features on or off, design-by-default, should be with the ISS, not users without contextual limitation or understanding, i.e. permission for access the phone camera should be restricted to only during the ISS (game), and not when not. But asking for the same game, each time, is a burden.

37. Consent should be contextual and limited by clear purposes. Geolocation data collected from children which are necessary to use a game [eg: Pokémon GO[7]], should not by default mean consent to be used for targeting marketing and tracking.

38. Apps used in the public sector ecosystem should never permit in-app marketing. ISS likely to be accessed by and directly by a child should not include advertising nor use their personal data for marketing or product development and promotion.

39. A kitemark-type system could be beneficial to ease children's and parental understanding where a trusted third-party body has undertaken the assessment, akin to the Soil Association system, or PEGI-style ratings for example.

40. Biometric data are commonly processed for accessing online tools but rarely meet the high bar of necessity. Use should be exceptional. Where a necessity test is met, every processor of biometric data from children, should be required to register as a processor

[7] Pokémon GO https://pokemongolive.com/en/

of such, with the ICO. The Protection of Freedoms Act 2012 does not cover children in Scotland and Northern Ireland, but should be extended to do so at the earliest opportunity. Regulators should be aware that (e.g.) on-device fingerprints and other biometrics are not necessarily shared with an ISS, but instead likely remain on the device for the device's own purposes (e.g. authentication).

41. Deception and covert data capture should be exceptional, not routine, and transparent in any Data Protection Impact Assessment. The Norwegian Consumer Council set out in their report *Deceived by Design: "How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Rights to Privacy.*[8]*"*

42. Intrusion and inclusion factors must both be considered to offer benefits from the Code to as many children as possible. While the Code must have regard to the UNCRC, there is nothing to prevent it proposing that it also has regard to children and young people with special educational needs or disability within the meaning of the Children and Families Act 2014 and Code of Practice. This would be better inclusive of all children and the most vulnerable persons in line with other legislation, such as special educational needs and should ensure that the thinking in the Code is inclusive of all kinds of familial support and parent-child relationships, and seek to empower all children.

43. The Code cannot stand alone but must be accompanied by education programme for children, parents, school staff and others involved with young people in order to embed awareness of rights and responsibilities of data protection law in everyday practices, and encourage an awareness of collective social responsibility on privacy.

[8] Deceived by Design (4.1 Default settings -Privacy by default?)
https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Threats, Themes, and UNCRC summary reference

44. At high level, any data collection and processing must meet the tests of necessity and proportionality. However “proportionality” is commonly viewed in terms of utility (whether it enables or is a barrier to the aims of the ISS wants). For children a test of proportionality, should not be seen from the ISS or data processor or controller’s point-of-view, but from the rights of the child, and whether the data collection and processing is proportionate to any potential harm and interference with fundamental rights and freedoms. This is framed by the UNCRC in terms of human rights.

	Threats	Issue	Code relevance	UNCRC
1	**Advertising / Commercial exploitation**			Non-discrimination (article 2) States Parties recognize the right of the child to be protected from economic exploitation (Article 32)
2	**AV: Adults posing as children / Grooming / Stranger Danger**	This is sometimes cited as a risk to a child and why real-life personas are required online. But this cannot be mitigated by AV, since the adult can simply invent a child persona, and pose as their own age appropriate parent/guardian. Do not use AV to try to solve this. All forms of content filters are historically unreliable in the face of a capable opponent.		States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child’s welfare. (Article 36) Best interest of the child (article 3) Right to privacy (Article 16)

3	**AV: Excessive data collection for Age Verification purposes**	If AV results in large pools of children's identities stored with common ISS who already track use across ISS (ie Google) could a parent use Subject Access to find all their child's Internet visits and use over time?		Non-discrimination (article 2) States Parties recognize the right of the child to be protected from economic exploitation (Article 32)
4	**AV: Identification incl a need to be anonymous to parents**	Users need and want private channels for safe or confidential communication, for example of domestic violence or abuse, and for positive discussions about themes they cannot discuss elsewhere, without fear of repercussion from parents who may disagree with their lifestyle or exploration of subjects such as religion or gender.	Anonymity should be possible for children to maintain, and they choose to do so to develop their personality and characters to the full, to explore their development of self, and to enable and control a trusted conversation on topics that they may wish those who know them could not identify with the individual.	States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare. (Article 36)
5	**Care and Control**			Best interest of the child (article 3) States Parties recognize the right of the child to rest and leisure, to engage in play and recreational activities (Article 31)
6	**Chilling effect**	Children need to be able to be free to develop their full personality. Children need to be free to make mistakes and rectify them. But institutions are commonly imposing surveillance and personal data capture form children that are imposed without	For any ISS covered by the Code, Data Protection and Privacy Impact Assessments should be mandatory in new developments, and	Right to life survival and development (article 6) Right to be heard and involved (Article 12)

		consultation or the views of the children taken into account.	updated with a history of material edits, for product enhancements. Ie. DPIA should always feature in the development workflow of an ISS likely to be accessed by a child, and be publicly available. The threats and risks should be assessed specific to children and the assessment should demonstrate how the child's right to be heard was taken into account.	
7	**Data responsibility dependent on user memory to access the account set up as a child**	Such support cannot be dependent on the data subject remembering account details and need to offer alternative methods to verify a legitimate relationship with the account. This was supported in a recent High Court judgement, in which the judge noted, "The use of passwords and similar devices for internet security is a proliferating one in our modern IT-driven society. We are constantly told not to write any of them down. We cannot therefore be blamed if on occasion we do not remember those details."	Companies should for example, commit to not sell or transfer any personal data from the child. New data controllers should mena new notice and consent must be re-obtained. Data Subject Access must be supported for the lifetime of data processing. In order to be able to ensure the right to Data Portability can be enacted, an ISS should be transparent what mechanism it offers to do so, prior to and at the point of data collection.	Right to be heard (article 12)

8	**Data responsibility orphaned over time**	Data subjects, children and parents, can find that a service they once used has gone out of business, and it is no longer possible to find out who has responsibility for their data processing. For children and young people this may be very important, as data captured as a child, may have lifetime retention and lifetime consequences. Disclosing the data shelf life, and data security and customer support beyond product warranty, will be important as a safety feature of ISS which support IoT products, and that may have a shorter popular lifespan, such as some online gaming apps, than the user data they process.	Support might potentially end on a sunset date, such as January 1, 2025, or for a specific duration from time of purchase, not unlike a traditional warranty, but that should also be contingent on the end of the data processing. Such disclosures should be aligned to the expected lifespan of the data retention, and communicated to the buyer prior to purchase. For apps this may be online.	Right to be heard (article 12)
9	**Deception by parents implementing the ISS**	Deception should be avoided in principle, given that children's rights are to be promoted as a stand-alone right from that of their parents.	ISS must not be invisible to the user or data subject about whom data is collected (ie Guardian Gallery) even if used as a parental surveillance or safety control.	Right to be heard (article 12) States Parties shall respect the right of the child to freedom of thought, conscience and religion (Article 14) (Article 23) (Article 31)
10	**Deception by the ISS/ Institution**	Deception should be avoided in principle, by the ISS or institution / org	Companies (ISS) must not deceive children as to purposes of data processing	The right of the child to be protected from economic exploitation (Article 32)
11	**Participation**	Children risk being excluded if hard age verification is used to block access online. The best interests of the child must respect their participation rights, not only protection, or impose patriarchal moral authority based on any	In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or	States Parties shall respect the right of the child to freedom of thought, conscience and religion

		current political or ideological view.	legislative bodies, the best interests of the child shall be a primary consideration.	(Article 14) (Article 23) (Article 31) (Article 3)
12	**Policies are opaque and prevent understanding**	Terms and conditions and privacy policies are written to cover the ISS liability, not to aid user understanding. Can you replace terms and conditions — publish a “duty of care” what they will and won’t do	Can you replace terms and conditions — publish a “duty of care” set of principles which are easy-read and can stand alongside the legalese what they will and won’t do	Article 12
13	**Price discrimination**			Non-discrimination (article 2) Right of the child to be protected from economic exploitation (Article 32)
17	**Privacy per se is not the correct sole focus. It can enable other rights.**	Freedom of expression		(Article 14)
		Right to assembly		(Article 15)
		Right to confidentiality		(Article 16)
		Rights to develop free from interference		(Article 16)
18	**Systemic unfairness**	The power imbalance between ISS and children, and the public bodies that process data obtained from ISS must be reset..		Non-discrimination (article 2) States Parties recognize the right of the child to be protected from economic exploitation (Article 32)

19	**Transparency of data processing**	Children's data should not disappear from any visible way to manage rights or to remove consent for the child, especially if data are archived by the ISS.	Follow Guidelines on transparency under Regulation 2016/679 17/EN WP260	Non-discrimination (article 2) States Parties recognize the right of the child to be protected from economic exploitation (Article 32)
20	**Blocking data transfers, or timed use restrictions**	Some ideas how to protect children's data online, have very worthy intentions but are impossible in reality, not because of the device technology or a missing technology solution, but because there are simple human workarounds. For example, the concept of a screenshot prevention tool (often asked for by children) is simply undermined as soon as you point another phone's camera at the screen. Images online for some time, can have been copied and distributed without practical trace. Software that limits screen time is easily worked around by changing the phone's timezone settings. The Code should avoid trying to cater to this given its impossibility.	There is a recognised notion of "plugging the analog hole" which is based on fundamental misconceptions how tech works and that there is a technology solution. Business and political desires combined with core misunderstandings of technology can lead to legislation and industry practices that are counterproductive or fundamentally flawed in practice.	

Table 1.

Response to the ICO consultation questions

Q1. Appropriateness of proposed age brackets

45. Age brackets could suggest guiding principles but not firm age breaks which would require the ISS to know the age of the child and treat them differently the day after each birthday. Any age verification (AV) must be a minimum information approach.

46. The Principle of Data minimisation must be paramount in efforts to establish that the user is a child. Aim for an attribute check, not data collection. Otherwise the additional data processed may create additional and new risks to the user with unintended consequences.

AV necessitates a level of parental interaction that many children do not have. AV also assumes one user, to one device, and a single adult account holder, when children (particularly some of the most vulnerable, in care for example) may use a shared phone.

Q2. Views on the proposed age brackets

47. The proposed age brackets would be not at all appropriate if age groups were interpreted as a demand for an ‘age-banded Code’. In the Gillick judgement, (Gillick v West Norfolk, 1985) wider rights of the child and capacity, were considered of importance. “Parental right yields to the child’s right to make his own decisions when he reaches a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision."

48. Given that capacity and not age, is the important factor in whether a user is competent to make decisions and a recognised feature of children and the existing UK law, the Code should not use hard-edged age brackets to define hard boundaries of acceptable practice.

Q3 Comments on the list of areas proposed by Government

Consent

49. Delegating consent to an appropriate adult is not consent from the child. A service cannot know if a user understands the risks and benefits of data access. Information provided by the Data Controller and received by a user, is not the same as Informed Consent.

50. Companies should, for example, commit to not sell or transfer any personal data from the child. For avoidance of doubt, and because Terms and Conditions will have materially changed - the relationship will be with a new company, at the very least- after any sale or liquidation resulting in the transfer of children’s data, notice and consent are invalid, and must be re-obtained.

51. defenddigitalme suggests:

- a complete and explicit ban on so-called ‘tracking walls’, not as a prescriptive technology ban, but the principle that denies access to a service unless the child (user) accepts the user tracking conditions, and
- an explicit prohibition on the practice of excluding users who have ad-blocking or other applications and add-ons installed to protect their information and terminal equipment.

52. In order to be able to ensure the right to Data Portability can be enacted, an ISS should be transparent what mechanism it offers to do so, prior to and at the point of data collection.

53. IoT devices that link with an ISS must provide notice and/or request user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or

services that will process or link their personal data. If the lawful basis is consent for this processing, the device/ISS must be able to function without that data processing for consent to be valid.

54. Predetermined settings in shared and smart environments, e.g. public WiFi, hotspots, street and car sensors, and smart homes discriminate against children and their right to be heard in decisions about them, and their right to privacy. They often say, 'by using this service you consent to our terms and conditions'. Institutions tend to disregard children's rights in all these regards, especially in situations where the child cannot choose not to take part, such as travel in a city, and this assumed or 'deemed' consent is little more than a legal get-out.

55. The Norwegian Consumer Council's report *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Rights to Privacy*[9] found that default settings are used by many companies, including Facebook, Google and Microsoft to manipulate users, and to nudge them towards the most privacy intrusive options. The Council determined this was "unethical" and not in accordance with principles of data protection by default and by design.

56. Deception and covert data capture should be exceptional, not routine, and transparent in any Data Protection Impact Assessment. 'Deemed consent' should be recognised as not being satisfactory to meet the lawful basis of data processing by consent.

Data protection by design and default including data minimisation

57. The coverage of the Code should include the development phase of the ISS so as to have the meaning of Article 25 GDPR, Data Protection by design and default. For any ISS covered by the Code, Data Protection and Privacy Impact Assessments should be mandatory in new developments, and updated with a history of material edits, for product enhancements. Ie. DPIA should always feature in the development workflow of an ISS likely to be accessed by a child, and be publicly available. The threats and risks should be assessed specific to children.

Data minimisation: Anonymisation and product development

58. **Case study: ISS HegartyMaths.** Their retention policy is that all pupils' personal data is retained for 24 months from the end of the academic year in which the account was last active, or the cessation of the contract or the pupil leaving the school.

59. After 24 months from the end of the academic year where a user was no longer in the school's MIS, HegartyMaths will "anonymise" any personal data relating to a user so it is "no longer identifiable". This process is not made visible to the child or their responsible school.It is unclear how secondary use of these data then aid product development.

[9] Deceived by Design (4.1 Default settings -Privacy by default?)
https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

60. We believe for many ISS this is little more than a Data Protection law workaround to enable indefinite retention of children's personal data, while the children are unable to make Subject Access Requests. However, there is no way for them to know whether data has been made non-identifiable or not - and, as GDPR has reset the threshold of what is identifiable (and thus personal) data, it is likely that methods of de-identification and/or pseudonymisation previously used will be insufficient to make it *anonymous*.

61. That individual users' data is being retained suggests intent to process in future; linked, individual-level data is inherently identifiable and must be recognised as such.

62. **Case study: Century AI.** According to the UK company[10], "Students learn, are assessed and can complete homework on Century. ***CENTURY tracks each students behaviour – every click and mouse move*** – to learn how the student learns and provide each student with a constantly adapting, personalised path to mastery." We understand that this product was developed live in 23 pilot schools in England under individual contracts with each school. We have been unable to ascertain whether pupils and parents were asked for consent for the use of their personal data in this AI development from the schools or whether Data Protection Impact Assessment were completed, but we understand that schools using the software give pupils no choice whether to use the system or not. While the company tells us data are anonymised, this only happens after the identifying personal data are collected, and are used for product development. **Since the lawful basis for this kind of processing must be on a consent basis, or offer a Right to Object, the Code has an opportunity to make this clear to ISS developers, schools, pupils, and parents.**

Age Verification (AV), Privacy, and Identifying who is a child

63. "Age Verification is a narrow form of 'identity assurance' – where only one attribute (age) need be defined. The method by which this is done is not prescribed, but it would be perverse were the desire for privacy and protection to create more new databases and even more risk. And these issues have been solved before, replacing the ID card and scheme with Verify; that infrastructure is rolling out EU-wide, and can be reused."[11]

64. The intent of GDPR Article 25, "Data protection by design and by default" underpinned for children by Recital 38, should mean that data minimisation is a key principle in any AV mechanism. The Code should only require an ISS to consider childhood, rather than identify a particular child, unless where necessary and proportionate.

65. As Nick Pickles, Senior Strategist in Public Policy at Twitter said in evidence to the Lords Select Committee on Internet regulation, "*Age verification has become seen as the silver bullet to solving a whole range of problems*."[12] However it is not, and creates its own risks.

[10] Century AI https://www.century.tech/
[11] Age Verification as the new cookie law? (August 2017) Phil Booth http://www.infiniteideasmachine.com/2017/08/age-verification-as-the-new-cookie-law/
[12] The internet: to regulate or not to regulate? Hansard, September 11, 2018 [p9] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/the-internet-to-regulate-or-not-to-regulate/oral/89767.pdf

66. If AV requires more information to be known by the provider of an ISS, this increases the data processing risks, including privacy and data security. A default principle must be that any information processed for the purposes of Age Verification, must not be used for another purpose. Some of the most common concerns on AV in more depth were set out by the Open Rights Group in their BBFC submission, in April 2018.[13]

67. AV must avoid the promotion of a single provider becoming a centralised store of children's personal ID. For example, Facebook becoming the de-facto AV authenticator. The risk of this is that it incentivises companies to onboard children at ever younger ages and manufactures consent to the ISS terms, simply because the user wants to access the service, and creates a future consumer base for the for-profit company.

68. Parents often lie for children, and children often lie to workaround age controls. However, there is a risk that some attempt to prevent this by calling for a verified child AND adult identities, and proof of family link and in doing so, create centralised data stores of ever more sensitive data.[14]

69. Privacy can be an enabler to other rights, and the rights of the child should have primacy in this Code, not the parent.

- Freedom of expression
- Right to assembly
- Right to confidentiality
- Rights to develop free from interference

70. In shaping this Code the Commissioner should be clear whether it is in their remit and aim of this Code to prevent children lying, or to protect their vulnerabilities from abuse and misuse by bad actors when they do?

71. AV principles should where necessary at all, advocate for:
    1. Verification of age as an attribute
    2. Child rights to privacy in
        a. the online world (from the profiling and/or use of behaviours and identity that only the ISS see)
        b. offline identity (the ISS having a permanent link to offline name, profile or identity)
    3. Autonomy of the child

72. AV principles should prevent or mitigate:
    1. Full identification or profile capture
    2. Parental rights competing with the rights of the child
    3. Anonymisation of data post-capture, often used as a workaround to avoid DP law, often badly done

[13] Open Rights Group BBFC consultation https://www.openrightsgroup.org/assets/files/pdfs/consultations/ORG_BBFC_DEA_Consultation_Response.pdf
[14] Google Family Link for Under 13s: children's privacy friend or faux? http://jenpersson.com/google-family-link/

73. Contextual integrity is often lost about how, when and why data are gathered for a specific purpose at the time of collection. Data provenance is rarely available. Any data that the ISS can provide to the child, under Subject Access, should demonstrate their source, and be able to provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the ISS and/or device including the ability to reset to the “factory default.”

AV and data privacy and protection by default: Parental threat

74. One unintended consequence of using AV done badly -- i.e. if it results in large pools of children’s identities stored with common ISS who already track use across ISS (i.e. Google) -- could be parents using Subject Access to see their child’s Internet visits and use over time. Where children and parents disagree over religious, gender, or life choices, it could create risk. Similarly, parents should not be able to use Subject Access to find estranged children.

Applied AV in ISS in practice

75.
    A. All AV techniques are circumventable
    B. multiplying or combining them will leave them still circumventable, whilst reducing usability and practicality still further.
    C. some techniques may have significant collateral impact upon systems which defend us against payment-card fraud
    D. some techniques involve the creation of large and sensitive databases which may be repurposed for monetisation, e.g.: advertiser web-tracking, data mining, etc.
    E. clear necessity and proportionality when an ISS requires the identification of a particular child, versus recognising users may be in childhood.
    F. Any AV technique must seek to minimise risk and decentralise, not consolidate, all the data in one place into a single source.
    G. AV should identify that “this person has met the threshold” not hold the data to prove you are what you say you are.

Case study of AV in current practice: Young Scot

76. We cannot recommend or support this AV model as appropriate for expansion. Young Scot is a national information and citizenship organisation supported by the Scottish Government for young people aged 11-26 in Scotland. The Young Scot National Entitlement Card is available free of charge to everyone aged 11-25 living in Scotland. It is presented as a Rewards Card, to use “for money off the things you love, exclusive rewards, proof of age and much more.”

77. The Young Scot card is part of the accredited national proof of age card scheme PASS. The UK’s national proof of age accreditation scheme is endorsed by the Home

Office, the National Police Chiefs' Council (NPCC) and the Security Industry Authority (SIA).[15]

9 card issuers are PASS accredited:
4 UK-wide issuers (CitizenCard, MyIDCard, OneID4U, Validate UK),
4 English local authorities (Bracknell Forest, Essex, Milton Keynes, Southwark), and,
Scottish issuer Young Scot.

78. PASS was launched in 2001 following an initiative led by the British Retail Consortium (BRC) to provide a system of endorsement for card schemes. PASS is supported by six major trade bodies: Association of British Bookmakers; Association of Convenience Stores; British Beer & Pub Association; British Institute of Innkeeping; UK Hospitality and the Wine & Spirits Trade Association.

79. In some administrative areas in Scotland, children can use the card for cashless catering machines in school, interfacing with companies such as iPayImpact or Capita's online payment management solutions at East Lothian council, or ParentPay in Ayrshire.

80. Using the smart infrastructure behind the Young Scot NEC (national entitlement card), the partnership supports "wider ambitions" including the Scottish government's aims of tackling inequalities and reducing poverty across Scotland, Scotland's Digital Future Strategy, and Transport Scotland's Smart and Integrated Ticketing Strategy, and the Scottish Government's Online identity Assurance programme board, linked to proof of entitlement.

81. "Proof of entitlement" in England via Home Office checks, have led to withdrawal of services from young people, such as higher education funding, Student Loans, and Free School Meals. Such withdrawal checks are set out in School Census Guidance 2018-19.[16] Any Home Office AV service for children would likely to be seen as untrustworthy as a result.

82. While the former Minister for DCMS Matt Hancock reportedly said[17], "The move of data policy including digital identity policy to DCMS was done to unite policy over data whether it's within or outside government," he would be incorrect to think that for the public, the boundary between the two does not matter. The Home Office link to ID and eligibility checks is toxic to trust for young people, school staff, and other organisations since the 2016 school census expansion[18] revealed use of national pupil data for secondary purposes, namely immigration enforcement and to further the strategic aims of the Hostile Environment policy.

[15] PASS http://www.pass-scheme.org.uk/about-us/
[16] 5.3.4.4 'FSM' eligibility checking service
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741006/2018_to_2019_School_Census_Guide_convert_V1_3.pdf
[17] Computer Weekly, June 2018, GDS loses digital identity policy to DCMS
https://www.computerweekly.com/news/252442712/GDS-loses-digital-identity-policy-to-DCMS
[18] Defenddigitalme timeline of the 2016 School Census expansion https://defenddigitalme.com/timeline-school-census/

83. The Young.Scot and the Young Scot Rewards online platforms also capture demographic information about users such as age, gender, and interests if a child is logged into a Google or YouTube account.[19] This type of opaque data capture and processing should be avoided, and is not a model for similar organisations to copy, in their own website administration.

Case study: G-Suite (Google Classroom and Google Apps for Education)

84. Google accounts are verified as school accounts if the child is a G-Suite user given an account by their school. These can also enable the creation of a verified and identifiable parental / guardian link in the Google Classroom product. However, this consolidation of personal data and the power that the company already has and can accumulate about a user, given the common use of Google analytics across third-party ISS and data that Google collects and processes therefore, linked to the individuals' accounts.

85. This also has unintended consequences, that a child under 13 may have access to ISS without parental consent or oversight, as happens today, because the school passes Google the child's personal details, and parent email, directly from the school information management system, and the child's Google social log-in can then be used to create user accounts and access a wide range of other apps at school and at home, while logged into the G-Suite account, using the social log-in to create the new account, without parental oversight.

86. G-Suite accounts are ascribed to a child in school, both in primary and secondary schools across the UK. The child and parents have no real way to object, since the tool is the way the school has chosen to share documents with the child, assign homework, and staff and children can communicate via a school assigned gmail account.

87. The system is split into two parts: Core services, and Additional services. User personal information collected in the **Core Services** is used only to provide the **Core Services** like Gmail, Docs, Sheets, and Slides. Information from all Additional **Services** can be used to provide, maintain, protect and improve them, and for product development.

88. The G-Suite agreement schools are expected to enter into is enormous.[20] Terms and Conditions are explicit that If the Customer allows children under the age of 13 to use any of the Services, they must obtain consent to the collection and use of personal information in the Services, described in the G Suite for Education Privacy Notice.

89. For any child under 18, the Terms further state it is expected that the [school] customer will obtain parental consent for the collection and use of personal information for use of the Additional Services. Additional services includes YouTube which permits tracking,

[19] https://young.scot/5rights/articles/your-5rights/
[20] https://gsuite.google.com/intl/en/terms/education_terms.html and https://support.google.com/a/answer/6356441?hl=en

interaction with DoubleClick and other Google analytics, Blogger, and other applications.

90. Reality in practice, is that at best, if consent is asked for at all, consent is manufactured as a tick-box exercise. Better policies can contain a permissions page in the child's Admissions booklet which lists the Core Google Apps a school uses. But there is no real option to refuse or give free consent. Many policies at many schools do not tell parents which apps are in use at all.

91. Parents and pupils are required by schools to sign it off a Home-School ICT agreement which encompasses acceptance of all the terms and conditions set out by the school, but are not set out explicitly, and usually not by application.

92. These can include further systems such as web monitoring (usually set out as no more than "I understand my Internet Use will be monitored") and often a social media policy, agreeing not to bring the school into disrepute in public fora.

93. Given this bundled process and lack of consent as a legal basis, schools need to make a choice for the legal basis for processing.

    1. All additional services are off except Chrome Web Store & Google Search Console
    2. DoubleClick off by default

94. Here's what data G-Suite collects from children, and how it may be used, in Google's own Terms and Conditions:

95. **Information that we collect**
    We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like.

    We collect information in the following ways:

96. ***Information you give us.*** *For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo*

97. ***Information we get from your use of our services.*** *We collect information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services or view and interact with our ads and content. This information includes:*
    - ***Device information***

- *We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.*
- ***Log information***
- *When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:*
    - *details of how you used our service, such as your search queries.*
    - *telephony log information, such as your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.*
    - *Internet protocol address.*
    - *device event information, such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.*
    - *cookies that may uniquely identify your browser or your Google Account.*
- ***Location information***
- *When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and mobile towers.*
- ***Unique application numbers***
- *Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.*
- ***Local storage***
- *We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.*
- ***Cookies and similar technologies***
- *We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyse the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites.*

98. *Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. When information is associated with your Google Account, we treat it as personal information.*
99. *For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy.*

100. **How we use information that we collect**

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones and to protect Google and our users. We also use this info. to offer you tailored content, like giving you more relevant search results and ads.

We may use the name that you provide for your Google Profile across all of the services we offer that require a Google Account.

In addition, we may replace past names associated with your Google Account, so that you are represented consistently across all our services. If other users already have your email or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account.

When you contact Google, we keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.

Our automated systems analyse your content (including emails) to provide you personally relevant product features, such as customised search results, tailored advertising and spam and malware detection.

101. *We may combine personal information from one service with information, including personal information, from other Google services – for example, to make it easier to share things with people you know. Depending on your account settings, your activity*

on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

102. We will ask for your consent before using information for a purpose other than those set out in this Privacy Policy.

103. Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.'

Biometric data processing: Intrusion and Inclusion

104. Capturing biometric data, including keyboard use or screen patterns, data including video or photographs of the user, and using hidden sensors should be forbidden for children without consent, similarly to the Protection of Freedoms Act 2012. Such use should be exceptional and should need to reach a high bar of risk or crime, before personal data capture is permissible. Data shared externally, including logging and metadata should also be shared with the child, or family with respect for the child, in an appropriate manner and timing, dependent on the nature of the risk.

105. After all, the GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".

106. It is one of the "special categories of personal data" that can only be processed if:

- The data subject has given explicit consent; (rarely possible for children)
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the fields of employment and social security and social protection law;
- Processing is necessary to protect the vital interests of the data subject;
- Processing is necessary for the establishment and exercise of defence of legal claims; or
- Processing is necessary for reasons of public interest.

107. Eye tracking is an example of technology via screen use already employed in UK schools and universities.

108. While a technology may be deeply invasive and objectionable to some children, the same technology may be empowering to others[21] and is closely tied with purpose and intent of data processing. This is why the Code must not be prescriptive on technology, but intent.

[21] Eye Gaze in the Classroom http://www.inclusive.co.uk/Lib/Doc/catalogues/eye-gaze-in-the-classroom-2015-v2.pdf

109. Eye gaze technology may have therapeutic purposes. Eye gaze analysis tools can record the data of where and when a student looked during specific activities. This data can then be reported back in different ways to show various eye gaze behaviours. These reports and images can be saved for reference and record keeping, profiling the children and providing an invaluable assessment and teaching tool for teachers and therapists.

110. Eye gaze technology can also be used as the screen interface for children with extremely limited mobility, giving them control and autonomy.

111. An age appropriate design Code must therefore aim to be as inclusive as possible. Cognitive, hearing, input and sight related accessibility features of data processing should be considered.[22] Technology that is safe as well as innovative, should be enabling to all people with disabilities to enhance their quality of life as much as possible. Differences between intrusion and inclusion would be captured in a DPIA.

Data sharing

112. Purpose limitation derives from the second principle in the Data Protection Act, which provides that at the point of the initial collection of personal data, the purposes must be specified and lawful, and that subsequent use must not be incompatible with those purposes.[23] However users' expectations of data being used for a direct purpose, rarely include the assumption of secondary purposes by the user, and commonly include that assumed entitlement by the data processor or controller.

113. It is common for children's personal data to be processed by ISS for the purposes of company research, which generally mean product development. Where these include the capture of personal behaviour, and biometric data in particular, or where ISS operate without a screen, the data sharing can be hard to see or understand. Policies may mislead a user even with accurate statements such as Mattel's Hello Barbie's privacy statement, "*Your children's conversations are not used to advertise to your child*."[24]

114. It is only set out in the deep detail of the ToyTalk privacy policy[25] that ToyTalk, *"may also use, store, process, convert, transcribe, analyze or review voice recordings (along with text and transcriptions derived from the voice recordings) in order to provide, maintain, analyze and improve the functioning of the speech processing services, to develop, test or improve speech recognition technology and artificial intelligence algorithms, to develop acoustic and language models, and for other research and development and data analysis purposes."*

[22] Accessible Gaming Wish List https://www.specialeffect.org.uk/accessible-gaming-wish-list
[23] See Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitation (2 April 2013) WP 203, at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last visited 30 August 2013
[24] Hello Barbie Privacy Commitment http://hellobarbiefaq.mattel.com/privacy-commitment/
[25] ToyTalk Hello Barbie privacy policy https://www.toytalk.com/hellobarbie/privacy/

115. And that data may be shared as transcribed text.

"We will not share voice recordings with Mattel. We may, however, share certain transcripts or other text derived from voice recordings with Mattel, which will be used solely for the purpose of enabling Mattel to assist us in providing quality control and in improving and approving the scripting of the Barbie Products.

"We may share voice recordings and other personal information as follows (subject to any applicable COPPA requirements or restrictions) with vendors, consultants, and other service providers who need access to such information to carry out their work for us, such as vendors who assist us in providing and maintaining the speech processing services, in developing, testing and improving speech recognition technology and artificial intelligence algorithms or in conducting research and development or who otherwise provide support for the internal operations of the speech processing services (e.g. if we use the Bing Voice Recognition API in connection with the speech processing services, voice recordings and other performance data associated with the speech functionality will be sent to Microsoft)."

Data linkage

116. Data linkage is another area which sharing and selling may not adequately cover, but is a growing area of concern in terms of transparency and the implications for children's data protection and applied interventions.

117. The ISS, a service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service, may mean a web app, with which the data are connected to other non-ISS sources.

118. For example, while today a child in the UK may use a screen that tracks and processes their eye movements[26] connected to their use of an ISS, in future it could be combined with always on 360 degree cameras, as recently installed by ONVU[27] in a Birmingham Academy of Further education (14-18 year olds).[28]

119. The combination of these sources of personal data, may not only be based on ISS but be linked to data input or use of the ISS, through the use of eye capture and facial surveillance technology. Using technology to measure pupil engagement with on-screen learning is growing in China today, for example.[29]

[26] Using eye-tracking technology as an indirect instruction tool to improve text and picture processing and learning, Mason, L., Pluchino, P., Tornatora, M. Published in Wiley Online, 2015, https://onlinelibrary.wiley.com/doi/abs/10.1111/bjet.12271
[27] ONVU Learning's LessonVU system https://www.onvulearning.com/security-safeguarding/ (Sept 2018)
[28] UTC becomes first school with cameras in every classroom, Schools Week, July 2018 https://schoolsweek.co.uk/utc-becomes-first-school-with-cameras-in-every-classroom/
[29] One school's controversial use of AI tech in classrooms, The Educator, June 2018 https://www.theeducatoronline.com/asia/news/one-schools-controversial-use-of-ai-tech-in-classrooms/250271

Profiling and inferred data

120. Inferred data should not be used to covertly profile children. Today "*typing patterns on a computer keyboard serve as a ground for predicting person's confidence, nervousness, sadness, and tiredness. A particular feature of such inference is that highly sensitive data like a person's emotional state can be predicted from seemingly non- sensitive information, such as his keystroke dynamics."*

121. *"Until recently non-commercial advertisers had access to only limited data about their constituency. Now they have begun to exploit the same targeted internet advertising system used by commercial entities by mining the reactions and discussions on social media in real time and to aggregate data and, extract 'value' from these data, such as inferences about personality traits and likely voting behaviour of the electorate."*[30]

122. Information such as this, collected as a child, could have huge implications for a child's development, especially where it is used to nudge and change behaviour, and kept indefinitely, or shared with third-parties. Such measures should not concern a child, building on the principles of GDPR Recital 71.

123. On other forms of profiling for commercial marketing purposes we note and support the recommendations of the 5Rights submission to the consultation, which we will not repeat.[31]

Case study: profiling and inferred data in current practice in schools

124. Safeguarding software is directed at and directly used by a child in UK schools, but used by many children unknowingly. The intention of these software is to monitor every user's activity on the computer or device, separately from functions of filtering and blocking inappropriate content and capture their behaviour, including personal data, from which risk inferences are made.

125. Constant monitoring provides a screen capture that is always on, on a rolling basis. Keyword logging is routine in many of these systems' providers, and checking against a library of keywords, which are opaque and can be of up to 20,000 words.

126. Companies such as NetSupport DNA can now even enable the computer webcam remotely and covertly to capture an image of the [child] user. We believe this should be banned, as followed in the US from the court case Robbins v. Lower Merion School District[32].

127. Key providers of safeguarding in schools technology in UK schools vary widely:

AB Tutor

[30] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[31] https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/e21716d2de6b1a833d3421eb936f366e.pdf p16
[32] https://cdn.pacermonitor.com/pdfserver/6LZS7RA/57562339/ROBBINS_et_al_v_LOWER_MERION_SCHOOL_DISTRICT_et__paedce-10-00665__0001.0.pdf

Bloxx
C2K to school (Northern Ireland).
Impero
Fortiguard Firewall
iTalc / Veyon
LANschool/Lenovo
Lightspeed Rocket
NetSupport DNA
Securus
Policy Central Enterprise
SWFGfl
Smoothwall UTM
Viglen
Websense Cloud

128. Evidence from 4,507 of 6,950 schools using the SWGfL tools who carried out e-safety self-reviews, using the 360 Degree Safe tool in analysis carried out by Professor Andy Phippen, Plymouth University[33], shows that school staff are not equipped to deal with, or challenge the outcomes from, this technology.

129. "*However perhaps even more concerning is that the two weakest aspects are those upon which a school would be most reliant on understanding the nature of data protection and safeguarding within the school setting. If both staff and governor knowledge are poor (and in both cases averages are below 'basic' practice, indicating that a large number of establishments do not have either in place) there is little likelihood that the complex issues around data protection or safeguarding are well understood, and an effective challenge to senior management on these matters certainly cannot exist."*

130. There is evidence from our discussions with school staff that children have learned some of what will trigger the keywords and use this as a prank tool, or to bully and harass each other out of the classroom using staff intervention as the vehicle. By looking up content on-screen while a peer is logged in to a computer but away from the desk, a fellow child can search for something that gets the logged-in child hauled before staff and, in one case reported to us, the school safeguarding panel.

131. Often personal data are inferred from the data that are captured. From a search for "cliffs", some providers infer a suicide risk. From a search for "black rhinos", a child is a potential gang member. These are not suppositions, but real life examples that teachers have contacted defenddigtalme about with concerns.

132. One must consider that our internet history is not simply a list of actions, but a document that shows what we're thinking about, or a set of unconnected thoughts. Children think and act in ways that they may not as an adult. People also think and act differently in private and in public. These inferred data should not be covert and it is

[33] Invisibly Blighted, The digital erosion of childhood, Leaton Gray, S. and Phippen, A. (p56) UCL IOE Press (3 April 2017)

deeply worrying that such inferences from private online activity are made visible to the State and to third party companies, but not a child or their family, even when the data capture is at home.

133. Web monitoring of children and staff 24/7, 365 days a year included at home in personal space and in private time. Mark Donkersley, Managing Director, e-Safe Systems Limited[34]: told the Parliamentary Communications Committee, 11 October 2016,

134. *"Bearing in mind we are doing this throughout the year, the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is 24/7 and it is every day of the year. Lots of our incidents are escalated through activity on evenings, weekends and school holidays. Invariably, although the volume decreases, for example, during the six-week school holiday in the UK, the proportion of incidents which are very serious during that period is much higher."*

135. We believe these software are invasive at all times, but in particular should not be on in a child's private time, and outside school premises, even if using school provided equipment.

136. Published evidence is clear about which groups of children are most affected by Prevent according to CRIN (Child Rights International Network): *"Between March 2014 and March 2016, 3,105 people under the age of 18 were referred to Channel across England and Wales - accounting for 48 percent of all referrals during the period. Among these children, certain minority religious and ethnic groups have been disproportionately targeted by these measures. Nearly 40 percent of the children referred to Channel were recorded as Muslim in the figures and more than a quarter were recorded as being ethnically Asian."*

137. Rights Watch (UK) and Liberty are concerned that, despite broad policy statements of compliance with data protection and privacy rights, the operation of the Prevent strategy and the Channel programme on the ground does not demonstrate due respect for personal information and privacy.

138. "*From the case studies considered by RW(UK) in its 2016 report, 'Preventing Education?', it appears local authorities, schools, and police authorities may be operating some system of data collection and sharing which records a child's interaction with the Prevent strategy or the Channel programme. This could include formal referrals, informal information and events such as a police visit to a child's home. RW(UK) and Liberty have significant concerns about the rigour and compliance of such a system of data collection with both the specific requirements of current data protection laws and the Human Rights Act".*

[34]http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html

139. **We provided more evidence in detail on this subject to the Data Protection Bill committee in the preparation of the DPA2018, when a new safeguarding condition for processing[35] was added to the Bill at the eleventh hour, at Committee Stage. We believe that ISS should never routinely capture personal data covertly.**

Location settings and Tracking

140. Two separate aspects of location data should be considered in the Code. ISS that capture a child's real-world location, such as the physical cafe their Pokemon Go map interacts with, or that their wearable is designed to track, and the digital footprint a child leaves behind while accessing the ISS and the ISS can track across the online world, as the child moves through it browsing multiple locations.

141. Do Not Track settings become perversely disempowering if the user is misled in what they mean. If a user believes their use is not profiled and tracked across multiple online interactions, by setting their browser to Do Not Track, it may not prevent all such uses. TLS session resumption, cookies, and user fingerprinting (the pattern of the computer user's behaviour is retained, profiled and linked to the attributes of the hardware so as to be able to identify the user), mean that the intent of trying to empower a child by not being tracked, by resetting any 'in-session' tracking, by switching on and off again, is annulled in practice.

142. Instead the key intent of GDPR Article 25, "Data protection by design and by default" and underpinned for children by Recital 71 on profiling that "Such measure should not concern a child" should become the principles of the Code of Practice, rather than a prescriptive technology mechanism for how to do so. This should prevent profiling of children in line with Recital 71, in particular to analyse or predict aspects concerning the data subject's performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements -- in effect where the ISS benefits more than the child.

143. However, unless this is applied across the board, any bad actors who continue to use these methods will be able to distinguish and discriminate against some aspects of the user base positively and negatively. This user segmentation enables some to be treated more favourable than others, for example, for price discounts and discrimination.

144. If by default, a child is unable to proactively *switch on* the profiling features, and enable the system to remember the child's choice to be profiled because they believe that for them as an individual, the tracking may offer them a better deal, then the systems will inevitably discriminate less favorably against all child users. More favourable discrimination will be offered only to adult users.

[35] Briefing on web monitoring and keyword logging software in schools March 2018 https://defenddigitalme.com/wp-content/uploads/2018/05/Web-Monitoring-Briefing-defenddigitalme.pdf

145. However, if the aim of ending tracking is to end discrimination, this means the most fair conditions should be on offer to a child at all times. Fairness by default. Therefore it is vital that the principle of non-discrimination is applied at a highest level:

- ISS must not discriminate against children compared with non-child users, and
- ISS must not discriminate among the child user base, to offer more favourable terms and conditions to only some users based on any kind of profiling.
- ISS where there is no screen (IoT toys out of the box) must be delivered as Do Not Track by default and smart devices delivered 'dumb' out of the box.

Transparency

146. Transparency-by-default of the tool, (how it works, the purposes of the ISS) and the intent of the tool (why it does what it does, for the purposes of the user and the ISS), and of policy and any changes in it, should all be encouraged. Can you codify the ISS intent and how can you check they do what they say they will do, or are not doing, or what they say they will not, if logic or algorithmic decision making is opaque?

Communications and notifications from the ISS

147. The Code itself must be understood by parents and children if it is going to add value to their understanding and expectations of what good practice from ISS providers should look like. Scenarios of each kind of threat model, and their mitigation should be included in worked examples to make abstract concepts easier to understand.

148. Privacy notices for ISS likely to be accessed by a child, must have child-friendly privacy notices and written for an appropriate user age. The purpose of privacy notices today tend not to be designed for informing the user, but are to provide a level of legal protection from liability for providers.

149. Privacy Notice alongside Terms and Conditions, fail to inform users of changes of policy today, especially if they no longer use the service. An ISS should be required to publish the history of any material changes to its privacy notices for a minimum of two years. Best practices should include policy date stamping, and a summary of the effects of the changes made, as they materially affect the user.

150. An ISS must consider how to accommodate accessibility requirements for users who may be vision, hearing and or cognitively impaired to maximize access for young users of all physical capabilities.

Ratings and assurance

151. A trusted provider kitemark type scheme run well, could help bridge the gap between parental understanding and complex third party products and services. This could be along the lines of the Soil Association, and offer a trusted level of safety standards expected at a glance, having had human assessment before awarding the mark.

152. The weaknesses of such systems, are however, that they need oversight. And if this fails, trust in the whole scheme could be undermined, for example shown by the Red Tractor scheme for Assured Food Standards, under which only 1 in every 1000 farms that it certifies receives an unannounced visit from its inspectors. Serious animal welfare failings in some providers were reported in summer 2018[36].

Duty of Care

153. ISS providers could be expected to set out their own principles of a Duty of Care and be held to account if they do not meet their own standards. For example on intent, and easy-to-understand language about how personal data are used by the ISS.

Marketing

154. Public sector apps i.e. NHS and educational apps, should never permit in-app marketing, product or service promotion for remuneration, whether intended to be read by the child or related family account holder.

155. **Case study:** Class DoJo, a classroom app, links from its own webpage to an article from September 2016, How Class Dojo plans to Make Money having been freeware distributed to children through schools:[37]

156. *"Having connected parents and teachers, five-year-old ClassDojo is now beginning to turn its attention to the next part of its journey: monetizing the service. The company said it has no plans to sell advertising. Instead, ClassDojo is looking at selling educational content. With access to so many teachers and students, the startup is leveraging its distribution capabilities to spread educational videos to an audience of teachers and students on a level that's never been seen before."*

157. *"It's a huge distribution platform to reach parents," Don said. "We want to, In the long term, enable parents to be consumers for their child's education."*

158. Essentially it is a "freemium" model, in which users are given the basic tools to use the service, but for those willing to pay, more content is added to enhance the experience. The company can send marketing email to the parents of the child, who the school signed up.

159. There are plans for this model to be based off and tailored to, a user location, in future.

160. Children's data are processed in the US and outwith the EU Data Protection regime. This is a risk factor for protection of children's personal data, and potentially staff and even financial data. It is therefore unlikely this app can be used lawfully under necessary in the performance of a public task. Since schools should not apply a consent basis in school[38] in our opinion, this app is processing in ways incompatible

[36] Red Tractor accepts need for change as shoppers want more spot checks, The Times, July 30 2018 https://www.thetimes.co.uk/edition/news/farm-animals-tortured-under-red-tractor-label-rcbrhxqlm
[37] ClassDojo Wants to Do for Education What Netflix Did for Enter (Inc.) https://www.inc.com/salvador-rodriguez/classdojo-monetization-slack-classrooms.html
[38] ICO Performance of a public task or in the exercise of official authority https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

with the General Data Protection Regulation and how the law can be applied to ISS in education.

User burden including Extended Use

161. The burden of maintaining age appropriate design-by-default, should be with the ISS, not users. If settings should *forget by default* there is a risk that ‘good’ developers create multitudes of different interfaces that require the users to set individual levels of controls each time they open the app for a growing number of settings: data minimisation, do not track, restricted hours usage, camera access, microphone access, geolocation storage and retention.

162. If settings revert to default high once a child logs out or navigates away from a service it will create friction and frustration starting the app for example. It may mean a user will swipe a series of “accept” clicks and make poorer choices to remove the notifications and access the ISS in their haste to get started, than a single set of wise choices made by the human, and remembered by the machine.

163. Prescriptive and unavoidable user friction in order to break extended use, must avoid making the user experience frustrating and reduce users’ experience quality. This could have unintended consequences including for security (downloading patches that workaround the intended code), and even negative effects on mental health, not improving it as intended.

164. Friction that intends to force children to be conscious users may have unintended consequences that create new, or displace risks. There is an inherent conflict in the position whether children have the agency to make a longer-than-short-term decision about their phone, tablet, or application state. Can children meaningfully use a dialogue box that says "Yes, I want [PokemonGo] to be able to use [my phone camera] so that I can [catch a virtual reality Pikachu], and [importantly] Remember This Decision after I close the ISS / app / session?"

165. If children (or indeed: adults) are faced with poor, nagging user experiences which create friction and become a hassle to use, and are asked the same question again, they end up downloading an "easier to use" hacked-and-malware-ridden version of the software that does not, but instead steals their data, credit card information, uses their device as part of a botnet, etc. In short: making an application easy and desirable to use, is part of security. If you add "friction" people will pursue snake-oil applications to lubricate that friction.

166. Better would be that a degree of contextual limitation or understanding is set by default ie: permission for the ISS to access the camera means only during the game, but not when not.

Security of Communications and Data Processing

167. Children need to be able trust that company communications will be secure. As children are less aware of the risks online, they may be more easy targets of spear-phishing and spoofing, in particular where accounts are linked to parental credit card data.

168. End-user communications, including but not limited to email and SMS, should adopt authentication protocols to help prevent spear-phishing and spoofing. Domains should implement appropriate available technology (such as SPF, DKIM and DMARC) for all security and privacy-related communications and notices as well as for parked domains and those that never send email.

169. We should seek to ensure children's devices and associated applications support current generally accepted security and cryptography protocols and good practices, such risk assessments. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This includes but is not limited to wired, Wifi, and Bluetooth connections.

170. We should seek to ensure all IoT devices and associated software have been subjected to rigorous, standardized software development lifecycle testing including unit, system, acceptance, and regression testing and threat modelling, along with maintaining an inventory of the source for any third-party/open source code and/or components.

171. Generally accepted code and system hardening techniques should be employed across a range of typical use case scenarios, including prevention of any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project's inception through implementation, testing, and deployment. Devices should ship with current software and/or on first boot push automatic updates to address any known critical vulnerabilities.

172. **Case study: "**VTech gathered a lot of data about children via its Kid Connect app that was bundled in with many of the electronic toys it makes. Almost 650,000 children downloaded the app and used it in conjunction with VTech's educational toys." [BBC, January 2018]

173. **Case study: "**The Norwegian Consumer Council has uncovered serious security and privacy flaws in smartwatches for children. Strangers can easily seize control of the watches and use them to track and eavesdrop on children." [Norwegian Consumer Council, Oct 2017]

174. **Case study:** "Education website Edmodo promises a way for "educators to connect and collaborate with students, parents, and each other". However, 78 million of its customers had their user account details stolen. Vice's Motherboard reports that usernames, email addresses, and hashed passwords were taken from the service and

have been put up for sale on the dark web for around $1,000 (£700).” Quote, Matt Burgess, VICE. To date, we do not believe that UK teachers or pupils were ever informed of the accounts breach. [Ref: http://jenpersson.com/edmodo-tracks-teachers-students-data-breach/]

Responsibility for data rights of redress can be neglected by ISS over time

175. Data subjects, children and parents, can find that a service they once used has gone out of business, and it is no longer possible to find out who has responsibility for their data processing. For children and young people this may be very important, as data captured as a child, may have lifetime retention and lifetime consequences. Disclosing the *data* shelf life, and data security and customer support beyond product warranty, will be important as a safety feature of ISS which support IoT products, and that may have a shorter popular lifespan, such as some online gaming apps, than the user data they process.

176. Support might potentially end on a sunset date, such as January 1, 2025, or for a specific duration from time of purchase, not unlike a traditional warranty, but that should also be contingent on the end of the data processing. Such disclosures should be aligned to the expected lifespan of the data retention, and communicated to the buyer prior to purchase. For apps this may be online.

177. Support cannot be dependent on the data subject remembering account details and need to offer alternative methods to verify a legitimate relationship with the account. This was supported in a recent High Court judgement, in which the judge noted, “*The use of passwords and similar devices for internet security is a proliferating one in our modern IT-driven society. We are constantly told not to write any of them down. We cannot therefore be blamed if on occasion we do not remember those details.”* [39]

178. The Internet Society published an *Internet of Things (IoT) Trust Framework v2.5* in May 2018. They wrote, “*Core to addressing inherent security risks and privacy issues in data processing, is the application of the principles to the entire device solution or ecosystem. These include the device or sensor, the supporting applications, and the backend / cloud services. As many products coming to market rely on third-party or open source components and software, it is incumbent on developers to apply these principles and conduct whole supply chain security and privacy risk assessments.”*

179. We believe that some of their framing on Privacy, Disclosures & Transparency may be useful for the Commissioner to consider when developing the Age Appropriate Design Code of Practice.

Retention should follow existing DPA requirements

180. Children’s data should never visibly disappear entirely for the child, where data are stored year on year, a profile should enable access to historic or archived data held.

[39] Richmond vs Selecta Systems Ltd [2018] EWHC 1446 (Ch) Case No: C31BS071 https://www.bailii.org/ew/cases/EWHC/Ch/2018/1446.html

For example, a maths app, Mathletics currently hides data from the previous academic year, making it likely the child will remember to ask about its continued processing or retention. “Following the archiving of data, on-screen activity results and gold bars earned throughout the previous academic year will no longer be visible to students.” While it is possible for teachers, not students to make the choice over the archiving, the decision is time limited. For example Mathletics, “opt out option for 2017 has now closed.” http://uk.mathletics.com/archiving

Rights to Erasure

181. What does a right-to-erasure look like for a child and why is it different, from that of an adult? Consistent rights to erasure, delisting, and rectification should follow good DPA practices and uphold children’s rights, as adults’ rights.

182. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the ISS and/or device including the ability to reset to the “factory default.”

Q4. The meaning and coverage of these terms.

Use of Terms

183. Risk and harm are not absolute to children of the same age and capability, but contextual and do not stay the the same for any child across time, even within the same age bracket. Two fifteen year old children who are both able to recognise risks of sharing real location in a game, may still experience different risk and threat levels from any compromise of their privacy, should one of the children be at risk from an estranged parent, and the other not.

184. The technology per se should not be regulated and standards mandated, because for example, all uses of geolocation technology by ISS, may be using the same technology but with different intents, and can be the *intent* which may cause risk or harm.

185. Care is needed therefore not to make all encompassing statements on ‘location services’ suggesting that, the intent to enable tracking on a child’s phone is always nefarious.

Language

186. Language should be careful on its choice of terms. For example one word, seen through both lay and developers’ lens, which could be interpreted to have a specific meaning by ISS, such as “standards.” Definitions should make this clear. Communications on the Code itself should be available in multiple languages to enable accessibility not only by children, but also family members.

Exclusion of apps for counselling and preventive services

187. While the Code excludes such services, it should recognise that some of these may exploit some of children's most personal data and vulnerabilities and need similar regulatory attention. We are grateful to medConfidential[40] for these case studies to highlight the issues.

188. We also take the opportunity to point out failure to take accountable adequate measures to ensure fair processing and obtain informed consent from parents or children in new NHS programmes, such as the System C single child health record across six regions in the south of England in 2017. CarePlus Child Health software integrated 800,000 health records across 14 clinical commissioning groups (CCGs), five local authorities and six unitary authorities. See Annex 2 for the "privacy notice" which failed to inform anyone of data processing. Some data are self-provided through online screens in surgeries and similar.[41]

Case study 1: My Sex Doctor app

189. 'My Sex Doctor', which was promoted/endorsed by the NHS Apps Library from 2014 - 2015[42], is a suite of three apps "offering basic sex education. The app covers all aspect of human sexuality, from body changes to sex orientation, from flirting to abusive relationships, from masturbation to the various sexual acts, from STDs to contraception."

190. "The app comes in two formats, a 'Lite' version, for young people age 12+, where access to certain content[43] is restricted, and a 'full' version, for people 17+ providing access to all content." Both of these formats are "ad supported", with a third 'My Sex Doctor Plus' format where individuals can pay to remove the ads.

191. According to its author, following its inclusion in the NHS Apps library, the My Sex Doctor app was apparently "prescribed" by some GPs[44], and was being promoted to young people by other NHS sites, including My Health London[45]. This raised immediate questions as to whether the NHS should be endorsing and promoting any ad-supported apps about sexual activity[46] to children, given the ability for ad networks to track users' usage and interests and serve adverts against those interests.

---

[40] medConfidential https://medconfidential.org/
[41] Freedom of Information Request to NHS England CCG regions in 2017 https://www.whatdotheyknow.com/request/childrens_data_system_c_careplus
[42] App My Sex Doctor https://web.archive.org/web/20140912030315/http://apps.nhs.uk/app/my-sex-doctor/#
[43] http://mysexdoctor.org/views/why-a-lite-and-a-full-app/ - the My Sex Doctor app is still available online in 2018, though not in the current iteration of the NHS Apps Library
[44] 25 March 2015, https://profile.theguardian.com/user/id/12790619?page=1
[45] https://web.archive.org/web/20150324004803/https://www.myhealth.london.nhs.uk/your-health/young-people/blog/my-sex-doctor-app
[46] NGO medConfidential has raised these concerns, and did not concern itself with the quality or content of the advice given, which they did not review. They presume any review of clinical accuracy performed by the NHS was limited to the accuracy of information provided to the user, and not to other issues.

192. Even more concerning, however, was the published commercial strategy of My Sex Doctor Ltd – to which the NHS had apparently paid no attention. Beyond the ads / ad tracking in the 'free' version of the apps, the company's "pitch deck"[47] explicitly stated of the app's users: "Once gained their trust we can leverage it for commercial purposes" (slide 11).

193. Apart from the silent withdrawal of the app from the Apps Library in or around July 2015, NHS England took no action to protect those individuals who took the NHS's endorsement of the My Sex Doctor app at face value; thousands[48] of young people who are now potential victims of a 'bait and switch' strategy to exploit them.

Case study 2: Institutional failures – NHS Apps Library

194. The original NHS Apps Library, launched on the NHS Choices website in 2013, was closed in October 2015, due to serious concerns about how many of the apps being promoted handled patients' data[49]. A new NHS Apps Library was launched in 2017, despite only one of the apps promoted being "NHS approved"– with two further apps marked "being tested in the NHS".[50]

195. It appears an artificial target or deadline may have been set, to ensure the new NHS Apps Library held 70 apps on the NHS' 70th anniversary; a snapshot from 1 June 2018 [51] shows just 49 apps in the Library, at least one of which has subsequently been removed. Only one further app was marked as "being tested in the NHS" on the 70th Anniversary, and no additional "being tested" or "NHS approved" apps appear in the current Library.

196. Despite a programme of work under the (now-defunct) National Information Board towards a more appropriate assessment process[52], as of September 2018 there are still serious issues with apps being promoted under the NHS 'brand'. These include significant problems with ad tracking, third party usage and unlawful 'consent' – notably the Public Health England 'One You' apps, in particular 'One You Couch to 5k'[53], but also many others being promoted to young people around healthy lifestyles, mental health and self-harm.[54]

197. Worryingly, the vast majority of the (unbadged) apps in the Library meet only "NHS quality standards for safety, usability and accessibility" – with no mention of, or way for people to determine, the NHS' assessment of apps' "Evidence of Outcomes", "Data Protection", "Security" or "Technical Stability" as per the Apps Library's assessment

[47] https://www.slideshare.net/FabrizioDolfi/my-sexdoctor-pitch-deck-43296908
[48] Google Play store reported around 20,000 installations of the NHS-promoted MSD apps by mid-2015
[49] https://www.computerweekly.com/news/4500255254/NHS-Health-Apps-Library-to-close
[50] https://arstechnica.com/tech-policy/2017/04/nhs-digital-apps-library/
[51] https://web.archive.org/web/20180601064354/https:/apps.beta.nhs.uk/
[52] https://apps.beta.nhs.uk/how-we-assess-apps/
[53] See, e.g. an assessment of the many failings of the app by Data Protection expert, Pat Walshe: https://threadreaderapp.com/thread/1035529376278958080.html
[54] The Apps Library's 'Student Health app' sends young people to http://www.expertselfcare.com/, which offers a free app providing "information and support for students who self-harm and may feel suicidal".

questionnaire. The NHS continues to endorse apps that are privacy-hostile, and potentially even unlawful, with no indication of the risks that they may involve.

198. While not specifically targeting children, "mothers meet up" apps like 'Peanut'[55] collect and share users' Facebook Friends lists, photos, and locations with third party applications. This is not mentioned on the NHS Apps Library top-level page (just that you can "*sign in to the app using your Facebook or Google account*") nor on the app's own sign up page. Instead, the information is buried in the company's privacy policy[56]:

199. "*When you register or login to the App using your Facebook account, you are authorizing us to access certain Facebook account information, including information you make available via Facebook,* ***your friends list, current location and those friends you have in common with other Peanut users.*** *Your Peanut profile and other information you make available via the App, including information you provide directly or indirectly through Facebook (i.e.,* ***your Facebook photos, your name, age, approximate location, friends you have in common*** *with other Users and other profile information),* ***may be viewed and shared by Users with individuals who may or may not be Users or via third party applications****."*

200. In effect, mothers sharing any pictures of their children on Facebook are deemed to have given permission for this app to then share those images with unspecified third parties, for unspecified purposes.

201. When designing to protect children, one must clearly also consider the choices and behaviour of their parents.

202. It was systemic 'leakages' of personal data such as this that forced previous iterations of the NHS Apps Library to be closed down. Peanut is a classic example of an app that should fail the current NHS 'Developer Assessment', and that would indeed have failed to meet even the previous Apps Library's published criteria.

203. Clearly the new assessment process is failing, or failing to be applied properly, for apps with dodgy and potentially unlawful behaviours that the NHS continues to actively endorse and, along with other health bodies, promote to the public.

204. It remains to be seen whether the new Secretary of State's enthusiasm for technology will result in even more pressure to be seen to be offering apps, or whether NHS England, Public Health England and others will – after five years of failure, and at least two separate attempts – begin to take seriously the need for everything that it promotes to patients of all ages to not only be clinically safe, but also clinically effective, protective of data and privacy, secure and lawful.

[55] https://apps.beta.nhs.uk/peanut/
[56] https://www.peanut-app.io/privacy

Q5A. Opportunities and challenges in setting design standards

205. Ranum's Law, "You can't solve social problems with software," should be a guiding principle in the Code. Over prescriptive technical standards or restrictions should be avoided, as they will be worked around, or soon become dated. Behaviour and intent are more important to focus on and solutions and mitigations of harm and discrimination, transferable across technologies and different cultural values. Using technology solutions to fix other technology risks is likely to be a flawed approach.

206. Technology changes, threats less so. Therefore the Code should not proscribe or define an acceptable practice for each technology feature, but rather a higher level of expected practice in the ecosystem to mitigate a threat ie: permission for the ISS to access the phone features during the game, where the access is necessary and proportionate for the ISS, but not when the user is not using the ISS, becomes the default age appropriate design.

207. The Code must not try to be a parent, patching gaps in social and educational understanding in lieu of parental interventions. But questions in the Code should always consider whether whether:
    - Do children have the ability to opt in to controls, or
    - Do adults opt-out of controls-by-default?
    - Are the Age Appropriate features covert or transparent?

208. In effect the defaults that are positive to child privacy should be on by default. Those that are negative to risks and potentially pose risks to the child, off by default.

Q5B. How the ICO might use opportunities and address challenges

The definition of an ISS and in the context of leaving the EU

209. The definition of an ISS in the current EU Directive is under discussion and may change, and speaks again to why and the Code must set out expectations of behaviour and acceptable intent, rather than acceptable and unacceptable technology specifications. Close cooperation must be maintained with stakeholders shaping any new ISS definition.

Education for appropriate application

210. Although outside the remit of the Code per se, we believe a strong emphasis needs put on parental and child education, and involvement in the Code development and testing. Parental groups and civil society may offer a resource to talk to in this regard.

211. Without education of young people and their advocates, teachers and parents, it is unlikely that a Code will stand alone and be effective in better supporting children's rights.

212. Children must know what these rights are, and what is considered 'age-appropriate' in order to set their expectations, compare that with the reality of their experience, and know how to complain if their rights are not met, in order to achieve rectification and redress.

213. Any educational materials should not only be made available through state schools, since children can also be privately, and home educated. Parents are still the biggest influencers for the majority of children, but some of the most vulnerable children have none.

214. Older children too, at age 16 and 17 are not being offered consent choices consistent with their rights and that they can fully understand or feel free to object to, or opt out.

215. *"The rise of education data science as an infrastructure for big data analytics in education",* wrote Ben Williamson in Big Data in Education (2017)[57]*, "raises significant issues about data privacy, protection and the responsible use of student data. In a recent news article it was reported that the company Blackboard had conducted a massive data mining exercise on student data from 70,000 courses hosted on its learning management platform."*

216. In 2017 Jisc reported that it was, "*currently working with 50 universities in the UK to set up a national learning analytics service for higher and further education. This is the first time learning analytics has been deployed at a national level anywhere in the world, creating a unique opportunity for the UK to lead the world in the development of learning analytics."*

217. The learning analytics solution was being developed, "*in collaboration with commercial suppliers and the sector."* but young people are left out, or do not understand what they are agreeing to when asked for "consent" in these programs, or its potential future implications.

218. Education must consider rights to voice, participation, and exercise of rights and remedies for all appropriate ages

219. We support the House of Lords Communications Committee 'Growing up with the Internet' Report recommendation, that "*digital literacy should be the fourth pillar of a child's education alongside reading, writing and mathematics, and be resourced and taught accordingly.*"[58]

[57] Big Data in Education. The digital future of learning, policy and practice. Williamson, B. (2017) Sage
[58] Para 397, House of Lords' Communications Committee 'Growing Up With the Internet', March 2017

Survey evidence and why guidance must be clear for parents

220. We commissioned a survey through Survation of 1,004 parents of children age 2-18 in state-education in England, between 17-20 February, 2018. Full survey results are available online at Survation[59].

221. Only 27% of parents asked, trusted commercial companies to use a child's data collected in schools appropriately, and journalists are least trusted at 21%. Yet sensitive and identifying national pupil data at pupil-level, are given out to these third parties regularly, without parents' knowledge direct from school information management systems.

222. We also found that despite legislation in 2012, The Protection of Freedoms Act, which requires parental consent for use of biometrics and an alternative to be on offer; where biometrics systems are being used by their child in school, 38% of families were not offered a choice before use in practice.[60]

223. Biometrics are also being used for identification in some online services, directed at a child, and used directly by the child, in for-profit systems, and should be covered in the Code.

224. Parents and children are generally unaware of their rights, and are uniformed what they should expect, and how their rights can be enforced. Current Data Protection law is therefore failing in practice for children in schools in England. This Code must be understood by parents and children, as well as ISS and all players in their data ecosystem, to be effective.

225. There is an opportunity to appeal to companies and ISS to treat fairness and transparency be design, and public information / education as a consumer right and safety feature.

Q5C. Where the bar should be set for the proposed age brackets

226. A kitemark-type system could be beneficial to support children's and parental understanding where a trusted third-party body has undertaken the assessment akin to the PEGI ratings for example. This would enable age guidance, rather than hard edged age requirements.

227. Anonymous personas must also be possible for children of any age to maintain online.

[59] Survation State of Data 2018 survey Survation full data tables http://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables.pdf
[60] Defendidgitalme info https://defenddigitalme.com/wp-content/uploads/2018/03/StateOfData2018_infographicv10-1.pdf

Q5D. Examples of ISS design you consider to be good practice.

228. Unfortunately, there are few today, and any suggestions may change from one day to the next as a company may change its terms or practices frequently.

229. Digital safe spaces for very young children can be desirable (ie adult users are not knowingly permitted in certain primary age apps and games). And for any user these allow only pre-written controlled chat interactions using a pick-list of language to use between users. Unsuitable words are filtered and blocked by default. While this limits Freedom of Expression, within the game (such as Animal Jam) this meets children's fair expectations.

230. We have seen apps in the education sector which apply an API with school information management systems to verify an account, rather than extract personal excessive data. There is good practice, but often over collect sensitive data, such as SEND and ethnicity.

231. However, poor practice is more commonly brought to our attention. Apps used in the public sector ecosystem ie. NHS / educational apps, should for example never permit in-app marketing, product or service promotion for remuneration, whether intended to be offered to the child or related family account holder. Current Department for Education "cloud" app guidance[61] recognises, "this would be sensible to avoid" but does not ban this, and should.

232. In providing the cloud service, the default position should be that an ISS enters into a legally binding obligation not to serve advertisements or offer paid-for materials for products or services to any child, parent/guardian, or school staff users via the ISS or apps signed up to by the school on behalf of the pupil.

Q5E. Any additional areas

233. Consent should be contextual and limited as cookie law should be. Geolocation data collected from children which are necessary to use the game [Pokémon GO[62]], should not by default mean consent to be used for targeting marketing and tracking.

234. We believe that GDPR Article 80(2) should be supported to enable user reporting and resolution processes and systems, to help children understand and activate their rights and improve the ability to access advice from independent, specialist advocates.

235. The Internet Society published an Internet of Things (IoT) Trust Framework in May 2018[63]. Some of that framing on Privacy, Disclosures & Transparency may be useful

[61] DfE Cloud guidance (2014) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644845/Cloud-services-software-31.pdf
[62] Pokémon GO https://pokemongolive.com/en/
[63] The Internet Society IoT Trust Framework v2.5 (May 2018) https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

for the Commissioner to consider when developing the Age Appropriate Design Code of Practice.

236. The Society wrote, "*Core to addressing inherent security risks and privacy issues in data processing, is **the application of the principles to the entire device solution or ecosystem**. These include the device or sensor, the supporting applications, and the backend / cloud services. As many products coming to market rely on third-party or open source components and software, it is incumbent on developers to apply these principles and conduct whole supply chain security and privacy risk assessments*."

Q6. Contributing further in developing the content of the code.

defenddigitalme would be interested in contributing to future solutions focussed work. We welcome the intention of the ICO to test the Code and put it out to consultative review, to assess whether it is workable before any version would be made publically available and expected to apply.

Name Jen Persson
Email jen@defenddigitalme.com

Useful References

The Internet Society Internet of Things (IoT) Trust Framework v2.5 (May 2018) accessed Sept. 2018, https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

UN Convention on the Rights of the Child (UNCRC)
Adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with Article 49 https://downloads.unicef.org.uk/wp-content/uploads/2010/05/UNCRC_united_nations_convention_on_the_rights_of_the_child.pdf

ClassDojo Wants to Do for Education What Netflix Did for Enter (Inc.)
https://www.inc.com/salvador-rodriguez/classdojo-monetization-slack-classrooms.html

House of Lords' Communications Committee 'Growing Up With the Internet',
(March 2017) Para 397

Richmond vs Selecta Systems Ltd [2018] EWHC 1446 (Ch) Case No: C31BS071
https://www.bailii.org/ew/cases/EWHC/Ch/2018/1446.html

Youth Juries Report: 'The Internet on Our Own Terms'
Coleman et al (January 2017)
https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/2bc6968f3e8079fa49d15b8f8d131399.pdf

Disrupted Childhood, the Cost of Persuasive Design, 5 Rights, (June 2018)
https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/bb24215ada7264f0db4b3a0060e755b1.pdf

Response to Working Party 29 Guidelines on Automated individual Decision-making and Profiling for purposes of Regulation 2016/679[64] [download DDM response.pdf 234 KB] [65]

[64] Working Party 29 Guidelines on Automated individual Decision-making and Profiling https://defenddigitalme.com/wp-content/uploads/2017/12/20171025_wp251_enpdf.pdf
[65] Defenddigitalme response to the WP29 Guidelines on Profiling and Automated Decision Making (and Children) https://defenddigitalme.com/wp-content/uploads/2017/12/DDM_Response-to-Working-Party-29-Guidelines-on-Automated-individual-Decision-making-and-Profiling-for-purposes-of-Regulation-2016_679_v1.2-2.pdf

Annex

1. UNCRC (Selected articles with most relevance)

The Data Protection Act 2018 requires the Commissioner to take account of the UK's obligations under the UN Convention on the Rights of the Child when drafting the Code.

Every child has rights, whatever their ethnicity, gender, religion, language, abilities or any other status. The Convention must be seen as a whole: all the rights are linked and no right is more important that another. The right to relax and play (Article 31) and the right to freedom of expression (Article 13) have equal importance as the right to be safe from violence (Article 19) and the right to education (Article 28).

This might be applied in the context of setting design standards for the processing of children's personal data by providers of ISS by giving consideration to the four articles in the convention that are seen as special. They're known as the "General Principles" and they help to interpret all the other articles and play a fundamental role in realising all the rights in the Convention for all children. They are:

Non-discrimination (article 2)
Best interest of the child (article 3)
Right to life survival and development (article 6)
Right to be heard (article 12)

Article 2 states that States Parties shall respect and ensure the rights set forth in the present Convention to each child within their jurisdiction without discrimination of any kind, irrespective of the child's or his or her parent's or legal guardian's race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status.

States Parties shall take all appropriate measures to ensure that the child is protected against all forms of discrimination or punishment on the basis of the status, activities, expressed opinions, or beliefs of the child's parents, legal guardians, or family members.

Article 5 says States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.

Article 12 requires that states shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of

the child being given due weight in accordance with the age and maturity of the child. For this purpose, the child shall in particular be provided the opportunity to be heard in any judicial and administrative proceedings affecting the child, either directly, or through a representative or an appropriate body, in a manner consistent with the procedural rules of national law.

Freedom of Expression is the focus of Article 13. The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.

The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

For respect of the rights or reputations of others; or
For the protection of national security or of public order or of public health or morals.

Article 14 States Parties shall respect the right of the child to freedom of thought, conscience and religion. States Parties shall respect the rights and duties of the parents and, when applicable, legal guardians, to provide direction to the child in the exercise of his or her right in a manner consistent with the evolving capacities of the child. Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect public safety, order, health or morals, or the fundamental rights and freedoms of others.

Freedom of Assembly is the subject of Article 15.

Article 16 is key on privacy. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks.

Article 17 of the UNCRC calls on States Parties to recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health.

17(d) Encourage the mass media to have particular regard to the linguistic needs of the child who belongs to a minority group or who is indigenous;
17(e) Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of Articles 13 and 18.

Article 18 States Parties shall use their best efforts to ensure recognition of the principle that both parents have common responsibilities for the upbringing and development of the child. Parents or, as the case may be, legal guardians, have the primary responsibility for the

upbringing and development of the child. The best interests of the child will be their basic concern.

Article 23(1) States Parties shall recognize that a mentally or physically disabled child should enjoy a full and decent life, in conditions which ensure dignity, promote self-reliance and facilitate the child's active participation in the community.

23 (3) acknowledges a need for such children to have the fullest possible social integration and individual development, including his or her cultural and spiritual development.

Article 29 States Parties agree that the education of the child shall be directed to:

- The development of the child's personality, talents and mental and physical abilities to their fullest potential;
- The development of respect for human rights and fundamental freedoms, and for the principles enshrined in the Charter of the United Nations;
- The development of respect for the child's parents, his or her own cultural identity, language and values, for the national values of the country in which the child is living, the country from which he or she may originate, and for civilizations different from his or her own;
- The preparation of the child for responsible life in a free society, in the spirit of understanding, peace,tolerance, equality of sexes, and friendship among all peoples, ethnic, national and religious groups and persons of indigenous origin

Article 31
States Parties recognize the right of the child to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural life and the arts.

States Parties shall respect and promote the right of the child to participate fully in cultural and artistic life and shall encourage the provision of appropriate and equal opportunities for cultural, artistic, recreational and leisure activity.

Article 32
States Parties recognize the right of the child to be protected from economic exploitation and from performing any work that is likely to be hazardous or to interfere with the child's education, or to be harmful to the child's health or physical, mental, spiritual, moral or social development.

Article 34
States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse.

Article 36
States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare.

2. NHS sample “privacy notice” for children’s data

South, Central and West Commissioning Support Unit for a new children’s data collection and processing system

SCW

NHS
South, Central and West
Commissioning Support Unit

Your child’s screening and immunisation information

On 1 April 2017 six small teams that look after screening and immunisation information for children in this region are combining into one single team. The new team will be part of NHS South, Central and West and will help health professionals get up-to-date screening and immunisation details about the children they are caring for in Bath and North East Somerset, Berkshire, Buckinghamshire, Gloucestershire, Oxfordshire and Swindon.

You and your child do not need to do anything differently, but if you have any questions you can ask your health visitor or practice nurse.

You can find out more about us, this change, and how we keep your child’s data safe at: **www.scwcsu.nhs.uk/chis**