**14 May 2019**

**To: CRC Committee**

**From: UNICEF East Asia and the Pacific Regional Office**

**Re: Draft Concept note on the CRC General Comment on Child Rights in the Digital Environment**

It would be helpful to frame the structure of the sub-headings around the cornerstone of international human rights law - the [principle of universality](https://www.ohchr.org/en/issues/pages/whatarehumanrights.aspx). As human rights are universal , inalienable, indivisible, inter-related and interdependent, it is important to emphasise that we cannot sacrifice one set of rights for another. For example, we must not compromise children’s right to access information, in order to protect them from harm.

Importantly, children’s rights are also human rights, and the whole international human rights framework applies to children, and not only the Convention on the Rights of the Child.

**Headings**

It would be good to add a first heading of access to the internet*,* which would cover inequality in access to the internet in for example rural areas, and in relation to gender, disability, ethnicity and immigration status. This would also address the difference between children who have access to the internet via computers and tablets with broadband or similar connections, and those who access the internet only via smart phones and sometimes with limited 2G coverage on a pay as you go basis. This is different from access to information, although connected in relation to the content accessible in these different contexts.

* Access to information and freedom of expression and thought
	+ It would be good for the General Comment to reiterate children’s rights in this area, and to emphasise that the International Covenant on Civil and Political Rights also applies to children. Recalling that Human Rights Council resolution 32/13 condemned unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and called upon States to refrain from and cease such measures; and further recalling the [Special Rapporteur’s 2017 report to the UN Human Rights Council](https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2017ReporttoHRC.aspx) which called on the private sector to mitigate State calls for censorship or surveillance to the maximum extent allowed by law, whilst also taking measures to ensure they do not cause, contribute to or become complicit in human rights abuses.
	+ This reminder of the existing relevant international legal framework would be helpful, particularly in the context of regions such as Southeast Asia where [civic space online is shrinking](https://bangkok.unesco.org/content/32bn-people-living-countries-where-civic-space-under-threat) and access to information is being restricted, which impacts on children as well as adults.
	+ A key area in which UNICEF is seeking to improve access to information online is in relation to access to sexuality education materials.
* Protection of privacy, identity and data processing

It is suggested that privacy should be sub divided into children’s privacy vis a vis (i) the public – e.g. covering the need for privacy settings and management of online identities; (ii) their parents or caregivers – noting that parental controls can be useful for use with very young children, but should be used in accordance with the evolving capacity of the child; and (iii) industry – calling for controls on collection of data by industry (see for example the [UK Children’s Commissioner report](https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/who-knows-what-about-me.pdf) into the collection and sharing of children’s data).

* Protection from violence, sexual exploitation and other harm

Protecting children from sexual exploitation online requires a multi-sectoral approach, which is set out in the WePROTECT Model National Response framework. It is also important to look at the digital technology tools used by the development and humanitarian sector to protect children such as the use of biometrics, and to [caution the collection of biometric data unless it is absolutely necessary](https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf).

**Specific Questions from the Committee**

* How can children’s views and experiences be expressed and taken into account when formulating policies and practices which affect their access to, and use of, digital technologies?
	+ It should be emphasised that there is a considerable divide between the understanding and use of digital technologies by children, and that of adults. This makes it even more important to frequently consult with children as technologies rapidly evolve to understand their experiences, and to formulate policies that take their opinions into account. It is also important for adults to continually check their assumptions about children’s experiences online against children’s lived experiences.
	+ There may be categories of risks which children may not have the capacity to understand, such as [company retention of data](https://techcrunch.com/2019/01/30/googles-also-peddling-a-data-collector-through-apples-back-door/); and categories of risk that children are better placed to understand than adults, such as online peer to peer violence and abuse.
* How can discrimination (originating offline or online) be effectively addressed, to ensure all children have their rights realised in a digital world?
* How should the General Comment treat the role of parents and other caregivers?
* How should the practices of businesses operating in the digital environment support the realisation of children's rights?
	+ Social media platforms, gaming companies, and websites, should be responsible for removing the worst forms of content that is harmful to children, such as content that encourages suicide, extreme violence, and sexual exploitation. Technology companies should also take responsibility ensure that algorithms do not reinforce searches by children for harmful content, as was highlighted in the recent case involving a [British girl who committed suicide](https://www.bbc.com/news/uk-47069865) after her Instagram feed reinforced her searches for suicide-related content. for States should consider imposing a duty of care on companies in this regard, as recently set out by the [NPSCC](https://www.nspcc.org.uk/globalassets/documents/news/taming-the-wild-west-web-regulate-social-networks.pdf).
	+ Businesses should follow the children’s rights and business principles. UNICEF and the ITU have produced a range of practical guidance documents and toolkits for business in this regard.
	+ Social media companies could support the UN by providing data on prevalence of reported violence against children online through their applications. It is understood that many companies collect and analyse this data but will not share it due to the commercial risk to their reputation.
* How can States better realise their obligations to children's rights in relation to the digital environment?
	+ States need to carefully balance children’s rights to protection, with their other rights to privacy, freedom of expression, and access to information. There are certain areas in which minimum State regulation should be imposed on the ICT sector as follows:
		- Retention and preservation of data by internet service providers to enable better investigation of cases involving child sex abuse materials. See further [ICMEC Model Legislation](https://www.icmec.org/child-pornography-model-legislation-report/) and global review.
		- Removal of known online content containing child sex abuse materials such as the [INTERPOL Worst of List](https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content).
		- Imposition of a duty of care on social media companies
		- Promotion of a free civic space online
		- Regulation of retention of children’s data by the private sector, especially biometric data.
* Is the realisation of children’s rights in the digital environment necessary to realise children’s rights in other environments?

Children’s online and offline worlds are increasingly overlapping and sometimes merging. As more educational content moves online and technology is used in classrooms, the internet becomes essential to children’s right to education and to access information. Further, as technology develops in relation to the internet of things children are increasingly interacting with technology in other environments such as at home (through toys, games, and home technologies such as alexa and robotics) and in public spaces (through public surveillance technologies and through publicly accessible toys and games). Further, the increased indefinite retention of children’s data by the private sector and governments means that children’s rights to privacy and sometimes identity are being affected across both space and time.

**Gender perspective**

It is important for the concept note and subsequently the General Comment, to acknowledge gender differences in the way boys and girls access and experience digital technology, and its related effect on children’s rights in a digital age and digital environment. We also believe attention should be paid to closing the digital gender gap for girls and boys (in access and use, self-efficacy, etc).

We suggest ensuring there is a gender perspective throughout the General Comment, but particularly in some key groups of rights (as the suggested structure for the GC) where the evidence shows that girls have different online and digital experiences compared to boys:

* Access to information and freedom of expression and thought: many girls don’t own phones or digital devices, or they are denied online activity as parents/ care-givers/ communities worry about their online safety, and or place less confidence in girls’ abilities to navigate the online world. In addition, girls face a range of social restrictions (or stricter oversight from adults), based on gender norms, when using digital devices and accessing online information. Content creation and self-expression is often driven by gender norms of feminine and masculine ideals; determines (or limits) platform choices; and online engagement can have gendered consequences (e.g. trolling, cyber-bullying) and experienced differently by girls and boys and gender diverse children.
* Right to education and digital literacy: the most compelling evidence of the impact of gender stereotypes around technology is the ‘self-efficacy’ gender gap, or the difference between girls’ and boys’ confidence and belief in their abilities. Girls have more barriers related to access and use of (digital) technology than boys, which is often because of lower levels of education and due to social and gender norms. Without equal access and use, girls can’t develop digital literacy in the same way as boys, i.e. by familiarising themselves with technology, developing same levels of skills and confidence to explore and benefit from the digital environment.
* Protection of privacy: girls and boys manage their privacy settings differently; girls have more concerns about their personal information online being exposed to risky situations; they are also more likely to suffer negative consequences from this than boys (e.g. non-consensual disclosure of nude photos appears to be a common practice that affects youths’ lives, and this is gender-based).
* Protection from violence, sexual exploitation and other harm: while this concerns both boys and girls, it is often more of a risk and a concern for girls; girls also experience a range of social restrictions which can mean that they are more likely to internalise ideas that phones can be unsafe or girls cannot be trusted with the phone, thereby further reducing their exposure to and benefit from the digital environment.

These gendered experiences also relate to how discrimination (originating offline or online) needs to be addressed, to ensure all children have their rights realised in a digital world. We recommend an input on how stakeholders can work to ensure that girls, boys and gender divers children have equal access to and use of technology, and that they are safe and secure when online.

**Recommended resources**

* Child Protection in the Digital Age, National Responses to online child sexual abuse and exploitation in ASEAN Member States, UNICEF East Asia and the Pacific, 2016.
* Girl Effect and Vodafone Foundation (2018). Real girls, real lives, connected. Available at<https://www.girlsandmobile.org/>
* Sey, A. & Hafkin, N, (EQUALS 2019): Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership. <https://www.itu.int/en/action/gender-quality/Documents/EQUALS%20Research%20Report%202019.pdf>
* GSMA Connected Women, 2018. A Toolkit for Researching Women’s Internet Access and Use. Available at <https://www.gsma.com/mobilefordevelopment/resources/a-toolkit-for-researching-womens-internet-access-and-use/>
* GSMA Connected Women, 2019. The Mobile Gender Gap Report 2019. Available at <https://www.gsma.com/mobilefordevelopment/resources/mobile-gender-gap-report-2019/>
* UNESCO Policy Brief – I would blush if I could (2019). Rationales and Recommendations for Gender Equal Digital Skills Education. <https://en.unesco.org/events/id-blush-if-i-couldclosing-gender-divides-digital-skills-through-education>

Including: UNESCO Think Piece 1 (2019). The ICT Gender Equality Paradox, and UNESCO Think Piece 2 (2019). The rise of gendered AI and its troubling repercussions