Companion Document to the OECD Recommendation on Children in the Digital Environment

OECD

This document was approved and declassified by written procedure by the OECD Committee on Digital Economy Policy on 24 January 2022 and prepared for publication by the OECD Secretariat.

Please cite this publication as:

OECD (2022), *Companion Document to the OECD Recommendation on Children in the Digital Environment*, OECD Publishing, Paris, https://doi.org/10.1787/a2ebec7c-en.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/DGP(2021)11/FINAL

Foreword

The *Recommendation of the Council on Children in the Digital Environment* ('the Recommendation') (OECD, 2021[1]), was adopted by the OECD Council at Ministerial Level on 31 May 2021. It was developed in recognition that the digital environment is a fundamental part of children's daily lives, and that clear guidelines and strong policy frameworks are needed to both protect children from any potential harm and to support them to realise the opportunities that the digital environment can bring. The Recommendation seeks to assist governments and other actors in implementing coherent policies and procedures that can empower children in the digital environment. It was accompanied by the OECD Guidelines for Digital Service Providers.

The Recommendation is the product of significant analytical work and consultation, and its drafting was guided by delegates to the Committee on Digital Economy Policy (CDEP) and to the Working Party on Data Governance and Privacy in the Digital Economy (DGP), as well as a multi-stakeholder informal group of over eighty international experts. Since the early stages of the drafting process it was recognised that the Recommendation would benefit from specific implementation guidance. This Companion Document seeks to meet that need, setting out background information and providing context regarding the fundamental aspects of the Recommendation and its applicability.

The Companion Document was drafted by Lisa Robinson and Andras Molnar (both from the OECD Secretariat). Elettra Ronchi (OECD Secretariat) provided overall guidance and feedback. The Companion Document was prepared under the aegis of the CDEP, with valuable input provided by delegates from both the DGP and CDEP. The support and the feedback of the international group of experts is gratefully acknowledged.

Table of contents

Introduction

Today, children spend many aspects of their lives in the digital environment, engaging with it through a variety of different devices – from smartphones and tablets to connected toys and Internet of Things (IoT) devices. They are enthusiastic users of social media sites, apps and video sharing platforms. They share personal data and user-generated content, and can come into contact with a wide variety of people and information. The digital environment offers real and important opportunities for children, such as allowing them to express themselves, acquire information and knowledge, and to socialise with peers. At the same time, the digital environment presents a wide spectrum of risks to which children may be more vulnerable than adults. It is important to support and empower children to realise the benefits of the digital environment, and it is equally essential to help them understand and address digital risks.

While zero-risk is unattainable, it is possible to establish the necessary conditions for a safer digital environment by providing children with the digital skills and tools to recognise and manage risks they may face in the digital environment, whilst also supporting them to realise its opportunities. Clear guidelines and strong policy frameworks are essential in achieving this, as well as in achieving enabling equitable access conditions for all children. This is particularly important as the opportunities and risks that children face in the digital environment cross borders and jurisdictions, and require international collaboration.

In 2021, following the review of the *Recommendation of the Council on the Protection of Children Online* (the '2012 version of the Recommendation') (OECD, 2012[2]) and in response to the rapidly evolving technological, legal and risk landscape, the OECD Council[1] adopted the *Recommendation of the Council on Children in the Digital Environment* (the 'Recommendation') (OECD, 2021[1]). The Recommendation recognises that the digital environment is a fundamental part of children's daily lives, and seeks to assist governments and other actors in implementing coherent policies and procedures that can address the delicate trade-off between enabling the opportunities that the digital environment can bring to children and protecting them from the risks. It is part of a broader body of Recommendations, guidance documents, and analytical work by the OECD on digital economy policy.[2]

Background to the Recommendation

The OECD's work on children in the digital environment dates from the 2008 Seoul Ministerial Declaration for the Future of the Internet Economy (OECD, 2008[3]), which called for a collaborative effort, "between governments, the private sector, civil society and the Internet technical community in building an understanding of the impact of the Internet on minors in order to enhance their protection and support when using the Internet". Accordingly, in 2011, the CDEP[3] released a comprehensive report which analysed the risks then faced by children on the Internet and the policies which were in place to protect them (OECD, 2011[4]). This led to the adoption of the 2012 version of the Recommendation.

The present Recommendation arose out of work to review the 2012 version of the Recommendation,[4] and revises it. It takes into account technological, legal, and policy advances that have occurred since 2012, and is the product of some four years' worth of analytical work and consultations. This analytical work included a survey[5] of Adherents to the 2012 version of the Recommendation; a comprehensive report providing an Overview of Recent Developments in Legal Frameworks and Policies (OECD, 2020[5]); and a Revised Typology of Risks (OECD, 2021[6]).

The Recommendation was agreed upon by consensus and informed by a multi-stakeholder process involving government policy makers, academia, business and industry, and civil society.[6] To support the development of the Recommendation, an Informal Group of Experts was formed, comprised of delegates from the OECD's Working Party on Data Governance and Privacy in the Digital Economy (DGP), representatives from relevant regional and international organisations, and leading international experts on the rights and welfare of children in the digital environment. Additionally, the delegates of the Committee on Digital Economy Policy (CDEP) (as well as DGP delegates) provided extensive comments and suggestions on various iterations of the Recommendation. The final draft version of the Recommendation was the subject of a targeted stakeholder and horizontal OECD consultation, which allowed for the voices of a wider group of experts to be heard.

Scope of the Recommendation

All OECD Recommendations are non-legally binding Acts of the Organisation, but practice accords them great moral force as representing the political will of Member countries. There is an expectation that Members and non-Members having adhered to them (the 'Adherents') will do their utmost to fully implement them.[7] Governments beyond OECD membership are encouraged to use the Recommendation to inform the development of their national strategies, whether they chose to formally adhere to it or not. In addition, all public and private organisations are encouraged to take account of its provisions when putting in place policies and practices designed to respond to the needs of children the digital environment.

The goal of the Recommendation is to find a balance between protecting children from risk, and promoting the opportunities and benefits that the digital environment can provide. It aims to help governments better address technological, legal and policy advances, identify tools that can continue to support children in realising the opportunities of the digital environment, and address the new and evolving risks that they may encounter in it. It highlights the importance of the shared responsibility of all actors in ensuring that the highly complex digital environment is both safe and beneficial for children. It recognises that governments have a key role in responding to the needs of children in this environment, that parents need support in fulfilling their fundamental role of protecting their children, acknowledges the essential role that Digital Service Providers play, and makes clear the importance of child participation.

It is also important to note that the Recommendation and the OECD's work in this area, complements the work of different OECD committees (including the Committee on Consumer Policy and the Education Policy Committee) and is part of a broader international dialogue with international organisations who have complementary work streams reflecting their specific mandates. As an illustration of the latter, the rights based guidance developed by the Council of Europe (COE) and the Committee on the Rights of the Child,[8] as well as the guidance developed by the International Telecommunication Union (ITU)[9] and the Global Privacy Assembly (GPA)[10]. Additionally, it complements guidance delivered on specific topics, such as on children's privacy in an educational setting,[11] on marketing practices,[12] or on responses to child sexual abuse material (CSAM).[13] The Recommendation acts to complement these actions, focusing on providing guidance to governments and on enhancing policy coherence. Additionally, as an addendum to the Recommendation, the OECD has developed Guidelines to Digital Service Providers (OECD, 2021[7]). These guidelines provide overarching guidance to service providers for children in the digital environment.

The Structure of the Recommendation

The Recommendation starts with a preamble (e.g. "Having regards", "Recognising", etc.), followed by clarification about terminology ("I. Agrees…"). Thereafter it includes numbered recommendations from the Council to governments and other stakeholders. These are divided into three main sections: (II) Principles for a Safe and Beneficial Digital Environment; (III) Overarching Policy Framework; and (IV) International

Co-operation. It then includes recommendations regarding the Guidelines for Digital Service Providers that were developed alongside the Recommendation ("V. Recommends…", "VI. Calls on…").

The preamble to the Recommendation recognises key factors such as, the complexity of the digital environment; the prominence of the need to protect children's privacy and personal data; the various roles of different stakeholders; and recognises other international work and instruments. In line with the United Nations Convention on the Rights of the Child, it defines children as "every individual below the age of eighteen recognising that different age thresholds may be appropriate in providing certain legal protections".

The first main section, (II) 'Principles for ensuring a safe and beneficial digital environment for children' is applicable to both public and private organisations who play an active role in setting policies and practices or providing services for children in the digital environment. These principles recognise the child's best interests as a fundamental value, call for measures which are proportionate, respectful of human rights and fundamental freedoms, foster both the empowerment and resilience of children (and of their parents and carers), and promote inclusion. They encourage multi-stakeholder cooperation, and child participation.

The next section is directed at governments regarding the need for an (III) 'overarching policy framework'. It calls for coherent policy, effective legal measures, and evidence-based responses. This section promotes digital literacy as an essential tool, and the adoption of measures that provide for age-appropriate child safety by design and responsible business conduct. The third main section deals with (IV) 'promoting international co-operation', highlighting the importance of countries collaborating through international and regional networks, including in the development of shared standards.

The last section recommends that Adherents promote the associated Guidelines for Digital Service Providers and calls on Digital Service Providers to respect these Guidelines when taking actions that may directly or indirectly affect children in the digital environment.

Since the early stages of the Recommendation's drafting process, OECD delegations have recognised the complexity of the subject matter and the need to facilitate the Recommendation's implementation by developing a separate document containing background information and explanations, and this document seeks to meet that need. This document is divided in two main parts. The first considers the context in which the Recommendation was developed. The second brings together the main concepts and elements of the Recommendation with supplementary explanation regarding the fundamental aspects of its provisions and their applicability.

Context: The evolving landscape

Children in OECD countries are more connected to the digital environment than ever before...

Over the last few years children's access to the digital environment reached unprecedented levels. Whilst in 2009, 85 percent of 15 year-olds students in OECD countries reported access to the Internet at home, this proportion rose to 95 percent by 2018 (OECD, 2019[8]). The increase in access might be even more significant than suggested by these percentages, as this measurement does not reflect the remarkable growth of mobile Internet access and the improvements in the quality of Internet services (Schleicher, 2019[9]).

…but children from disadvantaged backgrounds still need support to have widespread access

However, children's access to the digital environment is still disproportionately uneven among countries. Children may experience different kinds of barriers in accessing digital technologies based on their socio-economic and socio-cultural backgrounds. While in some countries home Internet access is almost universally available for 15 year-old children, in others it is significantly lower (OECD, 2020[10]). In addition, access can be inequitable within countries. Across the OECD on average almost all of 15 year-old students from advantaged schools have access to the Internet at home, compared to 90 percent of those who are from disadvantaged schools, with some countries indicating a much greater gap (for instance 94 percent compared to 29 percent) (OECD, 2020[10]).

With COVID-19 forcing over 1.2 billion students across the world out of school, the pandemic further exposed the profound disparities that still exist and the need to establish enabling and equitable conditions for all children (OECD, 2020[11]). This is especially important, if all children are to benefit from the access to information, cultural and educational materials, many of which are now only available in the digital environment (UNICEF, 2018[12]).

As has been noted by the OECD, to bridge the digital divide, improved digital infrastructure and connectivity is vital. Children need access to broadband services, and they also need to be connected well, which means access to high quality (and affordable) communication networks and services (OECD, 2021[13]). Although conditions to ensure physical access to the Internet are essential, they are however, not sufficient alone. It is also essential that children can access digital devices in ways that are appropriate for the intended use (e.g. searching for information, socialising with friends or doing their homework) (UNICEF, 2018[12]). In this regard, children from disadvantaged backgrounds may not only need to overcome physical barriers (such as poor infrastructure), but technological barriers. For instance, mobile devices with low functionality may limit their usability for children when they are using them to undertake complex tasks, such as writing or doing homework (UNICEF, 2018[12]). In addition, there are certain groups of children who may need to overcome barriers to accessing the digital environment as a result of cultural practices,

social norms, gender, and disability and minority status (UNICEF, 2018[12]) (T20: Task Force 4 Digital Transformation, 2021[14]).

Children engage with the digital environment from younger ages…

Children are increasingly connected to the digital environment from younger ages (Burns and Gottschalk, 2020[15]). Indeed, children tend to have their initial experiences with digital technologies before the age of two, in many cases even before they can talk or walk (Burns and Gottschalk, 2020[15]) (Joint Research Centre, 2018[16]). Providing screen media to infants has become a common parenting practice to occupy children when parents are busy with household duties or to calm infants down (OECD, 2019[17]). According to Common Sense Media, in the United States, children below the age of two are exposed to the digital environment as much as 42 minutes per day, 17 percent of which is on mobile devices (Common Sense, 2017[18]). In the United States and the United Kingdom on average 83 percent of five-year-olds use a digital device at least once a week, with over 40 percent using it every day (Burns and Gottschalk, 2020[15]). In addition, over the last few years there has been a significant increase in the Internet use of 0-8 year-olds, partly as a result of children using digital devices at younger ages (OECD, 2019[17]).

…and spend increasingly more time online

With increased access to the digital environment, children are also spending more time in the digital environment (Burns and Gottschalk, 2020[15]) as many now own smartphones, from which they can enjoy continuous connectivity (Smahel et al., 2020[19]). In addition, with the growing use of video platforms, an increasing number of children's activities, such as watching television, is gradually moving online (Smahel et al., 2020[19]). Across OECD countries, the time spent by 15 year-olds online grew from 23 hours per week in 2015 to 27 hours per week in 2018 (Burns and Gottschalk, 2020[15]) (OECD, 2019[8]). In Switzerland children's estimated time in the digital environment is 134 minutes per day, in France 146 minutes, and in Norway 219 minutes (Smahel et al., 2020[19]). Overall, over the last decade the average time that children spend in the digital environment doubled (or nearly doubled) in a number of countries, including in France, Italy, Germany, Spain and Portugal (Smahel et al., 2020[19]).

The digital environment is a fundamental part of children's daily lives and interactions and provides tremendous opportunities

The digital environment provides important opportunities for children, including for leisure, entertainment, or socialising with peers. Children are active users of social media, apps, streaming services and video sharing platforms. Across the OECD, 93 percent of 15-year olds reported chatting in the digital environment as one of their most frequent activities (Burns and Gottschalk, 2020[15]) (OECD, 2019[8]). In addition, in the United States for instance, 97 percent of teens aged 13 to 17 are active on at least one social media platform (Pew Research Center, 2018[20]) (Burns and Gottschalk, 2020[15]). Another survey of children aged 9-16 from 19 countries in Europe revealed that on a daily basis children's preferred activities include watching videos, playing online games, listening to music and communicating with friends and peers online (Smahel et al., 2020[19]). Children keep themselves entertained by watching and sharing video-content and TV programmes online. Research from the United Kingdom that examined the media use of children aged 5-15 revealed that children were as likely to watch TV programmes on any other digital device (such as tablets or mobile phones) than a television set itself (Ofcom, 2021[21]). The use of multiple devices often leads to "multi-screening". This means that children may use their tablet or mobile phone at the same time as watching TV (Ofcom, 2021[21]).

Children also use digital technologies for their education, to gain knowledge and information, and to develop their civic identity and engage in political issues (see below under "Children as Stakeholders"). The use of digital technology for educational purposes is widespread across OECD countries (OECD, 2019[17]). In particular, e-learning platforms are widely used by educational institutions to provide enhanced educational services for children (OECD, 2019[17]). These platforms can be used by schools to support the delivery of education in the classroom and to gain an enhanced understanding of students' learning needs (OECD, 2019[17]).

The digital environment may also pose a wide variety of risks to children

Along with technological and behavioural changes, risks have also evolved over the last decade and new ones have emerged. To take account of the changed nature of the risks that children face, the OECD adopted in 2021 a revised Typology of Risks which provides a high-level overview of the risk landscape in the digital environment (see below in Box 1).

Box 1. The OECD's Revised Typology of Risks

A number of new risks have emerged and the nature of existing risks have significantly changed over the last decade. New business models and technological advancements have contributed to changes in digital devices and services, which in themselves have contributed to the new risk landscape. In light of these developments, in 2021, the OECD revised its Typology of Risks.

The Typology of Risks presents a high-level and overarching overview of the different types of risks that children may face in the digital environment (see below in Figure1). The Typology identifies four risk categories, namely: i) Content Risks; ii) Conduct Risks; iii) Contact Risks; and iv) Consumer Risks. The Typology also identifies risks that cut across these four risk categories and can have significant impacts on children's lives. Specifically, these risks are: i) privacy risks; ii) advanced technology risks; and iii) health and wellbeing risks.

Figure 1. OECD Typology of Risks

Risks for Children in the Digital Environment				
Risk Categories	**Content Risks**	**Conduct Risks**	**Contact Risks**	**Consumer Risks**
Cross-cutting Risks*	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

Note: The Typology acknowledges risks that cut across all risk categories ("Cross-cutting risks"). These risks are considered highly problematic as they may significantly affect children's lives in multiple ways.
Source: OECD and Berkman Klein Center for Internet and Society at Harvard University

Whilst many of the risks that the OECD had previously identified in 2011 (underpinning the 2012 version of the Recommendation) are still relevant today (including contact and content risks), the revised Typology notes that many of the substantive acts underlying these risks have evolved. In particular, risks that previously existed, such as exposure to harmful content or cyberbullying have changed in nature, but still persist. There are various types of exploitation which may also pose risks for children in the digital environment (for instance the sexual extortion of children). There are also a number of new concerns which have emerged, for instance children acting in peer-to-peer exchanges where their own conduct can make them vulnerable (conduct risks) or the spread of mis or dis-information ('fake news').

Children today may face new types of fraudulent or misleading commercial practices. Children may also be exposed to potentially harmful marketing strategies blurring the line of what may be considered commercial content and what is not. Children may also be targeted with advertising based on the personal data that is collected from them, which raises financial, security, and privacy concerns. In addition, there are still instances of children being exposed to age-inappropriate and illegal products. With the abundance of personal information collected, processed and shared through advanced analytics such as predictive analytics and artificial intelligence, children's data may also be used for profiling, which may affect their fundamental legal rights and freedoms. The maturity and age of the child may impact their ability to comprehend the motivation behind this type of data collection and uses or the longer term privacy consequences. There are also increasing concerns on potential health and wellbeing effects of the digital environment on children, particularly on their mental health, although a stronger evidence base is required to further verify and address these risks.

Source: OECD Revised Typology of Risks (OECD, 2021[6]).

Key Concepts Underlying the Recommendation

The following sections consider a number of key concepts underlying the Recommendation and their meaning, highlights how these concepts have been incorporated into the Recommendation, and gives guidance on their practical application. The first section devotes special attention to describing the different key stakeholders and their roles. The second section elaborates on a number of key concepts which represent critical areas for policy action, namely, the concept of age appropriate child safety by design; safeguarding children's privacy; and the importance of digital literacy.

Stakeholders and their Roles

The Recommendation identifies 'stakeholders' as, "all organisations and individuals involved in, or affected by, the maintenance of a safe and beneficial digital environment for children" (at I.iv). 'Actors' are identified as a 'subset of stakeholders', and they are separately defined in the Recommendation as, "all public and private organisations who play an active role in setting policies and practices or providing services for children in the digital environment" (at I.i). These terms aim to capture all entities who, to varying degrees, have an impact upon children's interaction in the digital environment.

The different provisions of the Recommendation are directed at 'Adherents' (or governments), however all 'actors' are called upon to promote the 'Principles for a Safe and Beneficial Digital Environment' (at II) and the importance of engaging with all stakeholders is made clear in several places throughout the Recommendation. For example, the Recommendation encourages all actors to "engage in and promote multi-stakeholder dialogue" (II.5.a), that multi-stakeholder bodies be consulted in policymaking (II.5.b), and that governments coordinate the views, efforts and activities of stakeholders in the development of policies (III.1.c.ii). The Recommendation makes clear that children themselves, as well as their parents, are important stakeholders.

Below, the roles of the different key players involved in ensuring a safe digital environment and related recommended actions are considered. Whilst, a broader group of actors may be involved than those specified below, the section pays particular attention to certain actors and the roles that they play. This includes: *i)* governments; *ii)* children themselves; *iii)* digital service providers; *iv)* parents, carers and legal guardians; and *v)* teachers and educators.

Governments

As clearly highlighted in the preamble to the Recommendation, "Governments hold a key role in responding to the needs of children in the digital environment" (at Recognising 6). Through their policies and regulatory actions, they can help empower children to become confident and competent users of digital technologies, promote the benefits of the digital environment, foster the resilience of children, take proactive steps to reduce harms, limit children's exposure to harmful digital content and activity, establish a safer digital environment by design, and help enable equitable access to digital technologies.

Whilst Member countries who adhere to the Recommendation should respect it as whole, certain provisions seek to address limitations in government responses and policy making that were identified in the background analytical work underpinning the Recommendation, in particular concerns regarding *i)* fragmented policy responses, and *ii)* an inadequate evidence-base underlying legal and policy responses.

Fragmented Policy Responses

Arising out of the OECD's Overview of Recent Developments in Legal Frameworks and Policies (OECD, 2020[5]), it was identified that legislative responses to the needs of children in the digital environment is wide ranging and fragmented. It was observed that responses are largely made up of legislation aligned to specific risks, leaving the responsibility for meeting children's needs and addressing risks to those ministries or departments who would be responsible for doing so in the offline space. Whilst there is *prima facie* logic in such a response, in practice this can result in actions that are siloed, ignoring the reality that this is a space that crosses traditional legislative boundaries and with significant interdependencies. For example, the issues of sexting and cyberbullying requires a coordinated response from justice, health, and education (at a minimum) and consideration for the impacts on children's privacy rights. Consumer risks for children, may straddle both traditional consumer responsibility issues (e.g. enticements to spend on in-app purchases), and privacy issues (e.g. where data is mined from app-users). Additionally, by keeping legislative responses separate countries risk duplicating their efforts, overlooking important issues, and potentially creating new social issues arising out of a strict and at times indiscriminate adherence to laws (OECD, 2020[5]).

A similar fragmentation was observed at the level of policy. For example, whilst complementary policy actions and programs are necessary to fill gaps and address challenges, often such responses are scattered across sectors, leading to responses which are not coordinated between the different responsible authorities. Promisingly however, where governments establish single oversight bodies, issues arising out of the digital environment are addressed in a more targeted and coordinated manner (OECD, 2020[5]).

Accordingly, under the 'Overarching Policy Framework' section of the Recommendation (at III), a number of recommendations are designed to address the above concerns. Governments are asked to:

- Adopt clear policy objectives at the highest level of government (at III.1.a);
- Establish or designate oversight bodies (at III.1.b) which can:
  - Coordinate the views of stakeholders;
  - Meet policy objectives;
  - Review the effectiveness of policy actions;
  - Coordinate the actions of different government bodies, ensuring that such actions are cohesive and mutually reinforcing, rather than an accumulation of isolated or stand-alone (and potentially inconsistent) initiatives; and
  - Promote co-operation across borders;
- Ensure that adequate and appropriate financial resources are dedicated to implementing policy measures (at III.1.d); and
- Review, develop or amend laws, so that legal measures and frameworks:
  - Are fit for purpose, enforceable, and do not limit children's enjoyments of the their rights (at III.2.a); and
  - Provide effective remedies for children should they suffer harm in the digital environment (at III.2.b).

As noted in the Legal and Policy review, where countries have created an oversight body, this is promising in that it allows for issues arising out of the digital environment to be addressed in a targeted and coordinated manner (OECD, 2020[5]). Such oversight bodies should be both independent and properly

resourced. Nonetheless, it remains somewhat of a moving target as to how such bodies will operate in practice. For example, in the UK, the issue was considered in late 2021 through a parliamentary enquiry (UK Parliament, 2021[22]). Australia's eSafety Commissioner provides an example of an independent oversight body operating in practice. This national independent regulator and educator for online safety leads and coordinates efforts across different departments, authorities and agencies,[14] engages with international stakeholders, conducts research, provides education, prevention and awareness raising initiatives, and has the power to receive and respond to complaints (i.e. powers to issue take down notices as well as fines) (Australian Government, n.d.[23]).

Additionally, a number of recommendations are directed at addressing concerns that the narrow conceptualisation of laws, combined with a strict adherence to the letter of the law, can prove counter-productive and at times create new social problems for children themselves.

A prime example of this is the legal responses to sexting.[15] When children engage in voluntary sexting (which in itself is not necessarily harmful), they may be self-generating material, which could be legally classified as child sexual abuse material (CSAM), risking prosecution, criminal sanctions and even mandatory inclusion on a child sex offence register (which can have life-long negative impacts and consequences). Another example concerns situations where children may themselves be the author of harmful conduct (i.e. cyberbullying), and where a heavy reliance on a criminal justice response risks the criminalisation of young children (OECD, 2020[5]).

In response to these concerns, in addition to recommending that legal responses are fit for purpose and do not limit children's enjoyment of their rights (as noted above), the Recommendation provides that:

- Measures taken to protect children in the digital environment should be proportional, and not unduly punitive (at II.3.c); and
- Children are not unnecessarily criminalised, and educational and therapeutic methods for dealing with harmful behaviour be considered in the first instance (at III.2.e).

Inadequate Evidence Base

In addition to the above-mentioned concerns, the OECD's background analytical work also revealed significant gaps in measuring and monitoring the effectiveness of different legal and policy responses, as well as in the evidence base underlying such responses.

A lack of consistent approaches to definitions, methodologies, and indicators was seen, as were varied methods of monitoring the effectiveness of policies, with some countries not engaging in any monitoring at all (OECD, 2020[5]). It was observed that policy making for children in the digital environment is often impeded by inadequate evaluation of the impacts of existing policies, as well as by the use of unsubstantiated or partial evidence to justify a response that serves a particular political goal (Byrne and Burton, 2017[24]). Additionally, responses may be reactive in nature, with policy often more responsive to sensationalised media reports and high profile incidents, rather than driven by reliable and representative data (OECD, 2020[5]). For instance, there is a considerable mismatch between the public discourse and the evidence-base available when it comes to the possible effects of the digital environment on the health and wellbeing of children (OECD, 2021[6]). There is currently a need for comprehensive, good quality, large-scale studies on the health and wellbeing effects of the digital environment on children, particularly on mental health effects (OECD, 2021[6]).

In response, the Recommendation asks governments to adopt evidence-based policies by:

- Conducting regular impact assessments of laws and policies (at III.4.a);
- Encouraging and supporting research into the use of digital technologies and attitudes towards them, as well as on the benefits and risks of the digital environment (at III.4.b);

- Coordinating with all stakeholders (i.e. business, academia, civil society) to share and develop evidence (at III.4.c); and
- Ensuring that research is responsibly undertaken, in accordance with data protection principles (at III.4.d).

As seen above (at III.4.c) the Recommendation encourages co-ordination with various stakeholders in sharing and developing research. Whilst this provision covers a wide number of stakeholders, it is noted that it captures Digital Service Providers, who should (in accordance with the legal and regulatory framework under which they operate) publish their research for the purposes of regulatory oversight and transparency.

Additionally, in recognition of the inherently global nature of the digital environment, the Recommendation asks that governments cooperate at the international level, including by developing proposals for shared statistical frameworks, as well as for harmonised terms and statistical definitions of risks and benefits (at IV.2).

Children

Children are, of course, the most important stakeholders in this space, and the Recommendation calls on all actors to ensure that in all activities concerning children's participation in, or engagement with, the digital environment they uphold the child's best interests as a primary consideration (at II.1.a). In line with the United Nations Convention on the Rights of the Child, the Recommendation defines children as "every individual below the age of eighteen recognising that different age thresholds may be appropriate in providing certain legal protections" (at I.ii).

The Recommendation calls for inclusive responses and acknowledges the need for policy making to be sensitive to the different needs and vulnerabilities of different groups of children. In its preamble the Recommendation specifically notes that, "children's capabilities vary by age, maturity, and circumstances, and that actions and policies for children in the digital environment should be age-appropriate, tailored to accommodate developmental differences, and reflect that children may experience different kinds of access to digital technologies based on their socio-cultural and socio-economic backgrounds and the level of parental, guardian, and carer engagement" (at Recognising 4).

It is important to consider the role that children themselves play in ensuring that the digital environment is both safe and beneficial for them, and the manner in which the Recommendation seeks to foster their participation in this regard. It is well accepted that actively involving children in developing policies on matters that impact them can contribute to better policy measures. From a practical perspective, where children and youth are able to play an integral part in helping to develop programs and policies that will have an impact on them, it is more likely that they will be more aligned with children's needs, interests and backgrounds (Cortesi, Hasse and Gasser, 2021[25])

Article 12 of the Convention on the Rights of the Child provides that "States Parties 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". The Committee on the Rights of the Child has made clear that this should apply to both the individual child, as well as to groups of children. The Committee, has further stated that there should be a broad definition of 'matters that impact the child', noting that children should be included in the social processes of their community and society. Further, it is insufficient to merely listen to what the child has to say, where a child is capable of forming views, those views should be seriously considered (Committee on the Rights of the Child, 2009[26])

The Recommendation highlights the importance of ensuring effective child participation in several places. Notably, it calls on all Actors to:

- Uphold and respect the child's right to freely express their views and their ability, as appropriate considering their age and maturity, to participate in matters that affect them in the digital environment (at II.2.d); and
- To engage in multi-stakeholder dialogue, including with children themselves (at II.5.a)

Child participation can take a number of different forms. It could include engaging with a child individually regarding a matter that has affected them personally, for example being active in the formulation of redress or remedies when they have suffered harm as a result of activities in the digital environment, or ensuring that they are able to make autonomous decisions regarding their privacy when engaging with digital platforms (i.e. by requiring age appropriate information by default on the risks that the child could encounter in selecting different privacy settings). Child participation could also include ensuring that children are consulted in the formulation of policies (and/or in the research which underlies such policies), and embodying their views in outcomes and outputs. Lastly, it could imply involving youth voices in the development and design of the services themselves.

There are several examples of good practice relating to seeking the views of children with regards to understanding their experience of the digital environment. For example, Ofcom, the UK's communications regulator, runs an annual survey on media use, attitudes and understanding among children aged between and 5 and 15 years, as well as about the media access and use of children aged 3 to 4 years of age (Ofcom, 2021[27]). Likewise, the Australian eSafety Commissioner has run a survey of 8-17 year olds on their online safety behaviours and experiences, providing insights on how they deal with issues such as managing their social media, contact with strangers, sharing their personal information, and dealing with negative experiences in the digital environment (Australia, eSafety Commissioner, 2018[28]) Additionally, the CNIL (France's Data Protection Authority) in developing its Eight Recommendations to Enhance the Protection of Children Online (CNIL, 2021[29]) both conducted a survey among children aged 10 to 17 years to better understand their digital activities (CNIL, 2021[30]), and led a series of workshops with children and their parents. Notably, the workshops provided insight into how best to design digital interfaces so that children's rights are respected, and to better understand factors which can influence children's understanding of data protection issues taking into account their age, maturity and background (CNIL, n.d.[31]).

Another example of seeking the views of children through a survey is the #CovidUnder19 initiative, a global consultation survey organised by the United Nations Special Representative of the Secretary-General on Violence Against Children, in consultation with civil society partners. The survey sought to understand children's experiences of the pandemic, as well as their views on how to get involved in finding solutions to the global crisis. Some 26,000 children (aged between 8 and 17 years of age) from 28 countries participated in the survey. Whilst this survey did not focus solely on children's digital experiences during the pandemic, it provided useful information from the perspective of children themselves on how they felt about remote learning initiatives, and the extent to which children were able to gain access to the Internet when necessary (#CovidUnder19, 2021[32]) (Terre des hommes, 2021[33]).

A further international example is UNICEF's consultation with 245 adolescents (aged 12-19 years) across six countries regarding their perspectives on artificial intelligence (UNICEF, 2021[34]). Alongside this consultation, UNICEF reported on the methodology, indicating what worked well and what didn't to aid others in their consultations with children (UNICEF, 2021, pp. 22-24[34]). At the regional level, the European Commission (with the support of the EU-funded network of European Safer Internet Centres) ran the #DigitalDecade4YOUth consultation among some 750 children aged between 5 and 18 years[16]. This consultation sought to gain a better understanding of how the digital world impacts (the rights of) children and young people, what they themselves view as key opportunities and challenges, and expectations they may have for policy makers. The outcome of the consultation will feed into Digital Principles, including those related to children's protection and empowerment (European Commission, 2021[35]).

Also in the EU, the Better Internet for Kids (BIK) initiative brings together young people involved with national Safer Internet Centres across Europe, to represent the voices of the youth on online safety, digital literacy, and internet governance issues at annual Youth Panels. At these events, participants can share their perspectives with peers, agree on key themes, and prepare awareness raising materials (BIK Youth, n.d.[36]). Additionally, BIK Youth Ambassadors, worked together with stakeholders from industry and civil society[17] to develop a Youth Pledge containing commitments focussed on making digital platforms and services more age appropriate for children and young people (Better Internet For Kids, n.d.[37]).

The Digital Futures Commission in the UK has recently highlighted the importance of not merely doing research 'on children', or seeking to understand the 'impact of technology on children', but rather ensuring that research is conducted 'with' children, and that they are consulted as actors in their own right. In this regard, the Digital Futures Commission has, through collaboration with children's organisations and other experts, conducted consultations with children and young people with a view to understanding their experiences of engaging with digital technologies (Mukherjee and Livingstone, 2020[38]). The Council of Europe has also involved children directly in some of its own child-related standard-setting and decision-making procedures (Council of Europe, 2017[39])

In 2021, the Berkman Klein Center for Internet Society at Harvard University considered different ways that stakeholders can build participation models that can enable meaningful youth (12-18 years) involvement in the digital environment (Cortesi, Hasse and Gasser, 2021[25]). Box 2 below provides a brief overview of four such models highlighted by this research.

Box 2. Youth Participation Models

Youth Labs:

A youth lab is a (virtual or physical) space that bring together groups of young people with adult stakeholders to create opportunities to exchange knowledge. Youth labs require that the adults involved be excited, and able, to collaborate with youth, that there be a clear vision and thoughtfully designed program, and that there be actionable content that both the adult and the youth participants can work together on. Examples of youth labs include the '20 Minuten Youth Lab', which seeks youth views on media and on the work of the 20 Minuten website (20 Minuten, 2018[40]); and the Tages-Anzeiger Youth Lab, which likewise seeks to solicit children's views on the media (Tages-Anzeiger Youth Lab, 2021[41]).

Learning and Co-Designing Space

This is a collaborative and creative environment that brings youth together with experts so that they can learn from and with each other. These spaces seek to place youth at the centre of learning, design and advocacy, aiming to empower children to learn new digital skills and to co-design learning resources with other young people and the adults involved. Here, children have the possibility to learn new digital skills and to co-create content with experts and with other young people. The adults involved have the opportunity to engage in design processes with youth, and to develop materials that align with the interests, needs and experiences of youth.

Youth Board

Youth boards engage groups of young people with senior executives at the highest level of an organisation on strategic initiatives. This can serve to create a bridge between the organisation and the world of youth, leveraging their insights regarding future requirements for programs, products, services and processes. This both diversifies the perspectives that senior executives are exposed to, and allows for youth perspectives in decision-making at the strategic level, which may help inform policies, activities and programs that can empower youth and foster inclusion. Examples of youth boards, include the OECD's Youthwise initiative which brings together young adults aged 18 to 30 to discuss their hopes

and concerns related to the future of work (OECD, 2021[42]); or the World Economic Forum's AI Youth Council, which convenes young people aged 14 to 21 from different parts of the world to share their perspectives on AI ethics and governance (World Economic Forum, n.d.[43]).

Participatory Research

Participatory research models enable young people to participate as researchers in every step of the research process (from conceptualisation, developing a methodology, to the creation of outputs). This seeks to shift the focus of research from adults' perception of the experiences of children and young people to youth's actual experiences. Here, children are invited to connect research themes to their interests and experiences, to offer ideas on how data can best be captured, and to contribute to research outputs.

Source: Berkman Klein Center for Internet Society at Harvard University, 'Youth Participation in a digital world: Designing and implementing spaces, programs and methodologies' (Cortesi, Hasse and Gasser, 2021[25])

Digital Service Providers

The Recommendation defines Digital Service Providers ('DSPs') as, "any natural or legal person that provides products and services, electronically and at a distance" (at I.iii). Much like the digital environment itself, DSPs and the products and services they provide are wide-ranging and likely to continue to evolve over time. Today, they could be considered to include apps, programs, websites, search engines, social media platforms, online messaging services, online market places, content streaming services, online games, news or educational websites, community environments, and connected toys or devices. In some countries they could also include mobile and telecommunications operators.

As recognised in the preamble to the Recommendation, DSPs "*play an essential role in providing a safe and beneficial digital environment for children*". For example, social media platforms connect children with each other and can contribute to their social development. Children use apps, websites and online games for their education and leisure. Through the services they provide, DSPs can enable children to gain new skills, express their creativity in different forms, and explore new hobbies. They may also provide platforms for marginalised children or children with disabilities to explore their communities and find ways to connect with peers.

Nonetheless, as already noted, children can face a variety of risks in the digital environment, and it is often via the products and services that DSPs provide that children may be exposed to these risks. DSPs, therefore, play an essential role in providing a safe digital environment, and in developing technologies and establishing the conditions to safeguard children against the risks that arise out of the use of, and interaction with, their services. They can help to both develop (and encourage widespread adoption of) privacy protective, interoperable and user-friendly technologies that take into account children's age, maturity and circumstances, and which can help guard against hateful and harmful contacts as well as safeguard children's privacy. In this regard, DSPs should consider integrating children's rights considerations into their impact assessments, (see below in Box 3).

Box 3. Integrating Children's Rights in Impact Assessments

Integrating children's rights in impact assessments can guide Digital Service Providers in evaluating their policies and processes as they relate to their responsibility and commitment to support and respect children's rights (UNICEF, 2013[44]). By integrating child rights considerations into their impact assessments, Digital Service Providers take a significant step towards recognising children as stakeholders and rights holders, as well as towards understanding how their actions may directly or indirectly affect children (UNICEF, 2013[44]).

Such commitments by companies exist independently from State responsibility to respect human rights (UNICEF, 2013[44]), and in a number of countries governments have adopted processes for ensuring children's rights in their activities through impact assessments, for example in Finland, Spain, Sweden, Australia and New Zealand. (Digital Futures Commission, 2021[45]).

There are a number of international and national guidelines on rights in impact assessments. Whilst often these guidelines apply broadly, they encompass children's rights. Arguably, the most well-known framework is the 2011 United Nations Human Rights Council's "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy Framework" (United Nations Human Rights, 2011[46]). These Guiding Principles set out the relationship between business and human rights, including children's rights (Digital Futures Commission, 2021[45]).

In addition to these overarching principles, a number of guidance documents are explicitly designed to support businesses to integrate child rights' considerations in their business practices, through child rights impact assessments (CRIA). This includes guidance from the Digital Future Commission, Save the Children, UN Global Compact, and UNICEF. (Digital Futures Commission, 2021[45]) (UNICEF, Save the Children and The Global Compact, 2013[47]).

CRIA's generally take the form of a specified process, tool, or report which allows for the assessment of how a proposed policy or practice may impact the rights, needs and interests of children. Whilst there may be differences between the various CRIAs, typically they follow eight steps (Payne, 2020[48]) (Digital Futures Commission, 2021[45]):

1. A set of core questions that take a holistic approach to the child and children's rights;
2. Screening/initial assessment stage, whereby an initial check on the proposed policy is undertaken to determine if a full assessment is necessary;
3. Identifying the information available to undertake the CRIA;
4. Gathering data and evidence, and consulting with children and young people;
5. Conducting a full impact assessment (identifying both beneficial and harmful potential impacts on children's rights) is conducted;
6. Making recommendations regarding any modifications necessary to protect children's rights;
7. Identifying processes for monitoring and evaluation; and
8. Making results publically available, including in a child friendly version.

Additionally, as children's activities in the digital environment are the focus of commercial interests, and can result in a multitude of monitoring and data-generating processes, DSPs play a key role in protecting children against privacy risks and inappropriate commercial practices. As such, it is essential that they provide children (and their parents, guardians, and carers) with concise, clear and age-appropriate information on the way that their personal data is collected, disclosed, made available, or otherwise used.

The use of advanced technologies by DSPs (e.g. Artificial Intelligence, Internet of Things, predictive analytics, biometrics), can bring important benefits - but may also encompass risk components. For instance, profiling on dedicated e-learning platforms may negatively affect children's privacy (see below in Box 4)

Box 4. The benefits and risks of e-learning platforms

During the COVID-19 pandemic the availability of, and access to, e-learning platforms has been essential in allowing children to continue their education. E-learning platforms can be viewed as 'transformational' for parents, educators and children. Already before the pandemic, such platforms provided educational resources in different digital formats (e.g. video lectures accompanied by child friendly exercises) (OECD, 2020[49]). For instance, in 2018, on average across OECD countries almost half of all 15-year old students were attending schools, whose principal reported that an effective e-learning platform was available (OECD, 2020[10]).

Nonetheless, e-learning platforms may pose a risk to children's privacy as a result of the collection, use, reuse and disclosure of personal data (Hye Jung Han, 2020[50]) (OECD, 2020[11]). Whilst in some cases these uses of data are necessary to ensure the proper operation of the e-learning platform (and in turn meet children's educational needs), the merging of public education with for-profit platforms and business models has raised concerns (Livingstone, Stoilova and Nandagiri, 2019[51]) (OECD, 2020[11]).

For instance, a number of e-learning platforms have been reported to engage in unsound practices such as the service provider collecting information without consent, and allowing teachers to remotely monitor students without consent (Hye Jung Han, 2020[50]). In addition, the OECD has observed that e-learning platforms that use video conferencing services may lead to inappropriate data collection and privacy violations (OECD, 2020[11]).

The COVID-19 crisis further highlighted these concerns with not only lessons occurring through e-learning platforms, but student-teacher interactions potentially being conducted on apps and social networking platforms that may not have sufficient personal data protection and privacy safeguards (OECD, 2021[6]) (UNICEF et al., 2020[52]). To address these concerns (both pre and during the pandemic), a number of guidance documents have been released which focus on protecting children's data and fundamental rights (notably the right to privacy) in educational settings, including from the Council of Europe and the Global Privacy Assembly (formerly known as ICDPPC). These documents set out principles and provide recommendations for governments, data controllers and business (Council of Europe, 2020[53]) (ICDPPC, 2018[54]).

In recognition of the essential role that DSPs play, alongside the Recommendation, Guidelines for DSPs were developed. The Recommendation states that governments should promote the Guidelines (as well as their continued development) (at V), and calls on DSPs to respect them (at IV). The Guidelines are highlighted in Box 5.

Box 5. Guidelines for Digital Service Providers

The Guidelines are a holistic set of principles which seek to support DSPs in determining how best to protect and respect the rights, safety, and interests of children, when they take actions that may directly or indirectly affect children in the digital environment. They also promote governmental engagement with the private sector in supporting the realisation of the key principles in the Guidelines.

Specifically, the Guidelines:

- Encourage DSPs to adopt a child safety by design approach when designing and delivering services that are for children or where it is reasonably foreseeable that they will be accessed or used by them (at 1).
- Call for information provision and transparency, specifically through the provision of information that is concise, intelligible, easily accessible, and formulated in clear, plain and age-appropriate language (at 2).
- Make recommendations pertaining to the protection of children's privacy and highlight the importance of policies and procedures in place to promote the best interests of all children who access the services of DSPs (at 3).
- State that DSPs should comply with domestic policies, regulations, or laws in place to safeguard the rights of children in the digital environment (at 4).

All DSPs are called upon to respect the Guidelines as a whole, however the specific measures individual DSPs may be expected to take might vary significantly. Factors such as the national legal and regulatory context in which they operate in should be taken into account, as well as the differences in their roles and the risk profiles associated with the widely varied services and products they provide, to which any measures they take will need to be proportionate.

For example, the measures taken by a DSP offering a service explicitly directed at children that has been developed with child safety by design in mind (such as an early learning digital game which may have built-in safeguards preventing unwanted messaging and parental controls) may be very different from those expected of a DSP (such as a social media platform) offering a service which has a mixture of adult and adolescent users and an inherently increased risk that a child may be exposed to inappropriate or harmful material. Differences in the expected age cohort of users may also impact the nature of any potential risk and in turn the measures that may be taken to address such a risk.

Source: OECD Guidelines for Digital Service Providers (OECD, 2021[7])

The Recommendation also addresses the role of governments in regulating the activities of DSPs, and the role that DSPs play in policy-making. The Recommendation encourages the positive engagement of both business and DSPs in policy-making (at II.5.c). Additionally, in light of the reality already noted that it is often via the products and services that DSPs provide that children are exposed to risk or suffer harm in the digital environment, the Recommendation instructs governments to both:

- Put in place legal measures to promote responsible business conduct (at III.2.c); and
- Define, in their domestic legal frameworks, the conditions under which DSPs may be held liable for illegal activity by, or illegal information from, third parties using their digital products and services, which harm children (at III.2.d).

Parents, Carers & Guardians

Whilst it is undisputed that, in principle, parents hold the primary role of safeguarding their children's interests in the digital environment, the changing and rapidly evolving nature of technology can often leave parents (carers and guardians) in a space where they may not fully comprehend the technology or the risk, and therefore may not have the substantive capacity to fulfill this role. In the face of rapidly advancing digital technologies, it is often children themselves who seem to understand technology (although not necessarily the risks) better than the adults who have been entrusted to both keep them safe from harm in the digital environment, and to guide them on how to use technology in a responsible and positive way. For example, whilst it has been observed that parents may have higher digital literacy skills then their children aged 9-11, they are likely to have the same skill levels as their children aged 12-14, and weaker skills then their children aged 15-17 (Byrne, Kardefelt-Winther and Livingstone, 2016[55]). Additionally, not all children have a responsible parental figure, and as noted in the analytical work underlying the Recommendation, there are gaps in policy responses for children who are unable to turn to their parents for support in navigating the digital environment (OECD, 2020[5]).

In recognition of this the preamble to the Recommendation makes it clear that whilst parents have a fundamental role in protecting their children in the digital environment they need support in this role. Thereafter, throughout the Recommendation particular areas in which parents may need this support are specified. That is:

- In fulfilling their role of evaluating and minimising risks of harm, and optimising the benefits of the digital environment for their children (at II.2.a, II.5.d);
- In having an awareness of the rights of children in the digital environment, as well as mechanisms for enforcing those rights (at II.2.b);
- In understanding their children's rights as data subjects, as well as how their children's data is collected, processed, shared and used (at II.2.c);
- In understanding how to access remedies and services when their children require assistance as result of harm suffered via the digital environment (at II.2.e);
- In having an awareness of online commercial practices that may cause harm to children (at II.2.f); and
- In fulfilling their role in helping to ensure that their children can become responsible participants in the digital environment (at II.5.e).

Additionally, the Recommendation makes clear that parents are an important stakeholder and that they should be included in any multi-stakeholder dialogue regarding the needs of children in the digital environment (at II.5.a).

Already, in 2017 when the OECD conducted its survey regarding the implementation of the 2012 version of the Recommendation, engagement with parents was noted to be key. At that time, it was observed that a number of countries had programs in place to meet the digital literacy needs of parents, and to raise their awareness of the specific risks that their children may face in the digital environment (OECD, 2020[5]).[18] For instance, in France the Ministry of Education established "La mallette des parents" as part of its policy to educate parents about school teaching programmes, and issues such as cyberbullying, safeguarding children's privacy, and the use of digital devices in the classroom (O'Neill, Dreyer and Dinh, 2020[56]).

It is also important to ensure that parents (and indeed children) are not expected to take responsibility for the design of services, and that the responsibility for preventing and responding to online harms is not placed solely on the shoulders of parents. In this regard it is worth noting the Australian eSafety Commissioner's Safety by Design initiative (see Box 6), which seek to put the safety and rights of the user at the centre of the design and development process, making it clear that service providers have a

responsibility to prevent and respond to harm, and that the burden of safety should never fall solely on the user (Australia, eSafety Commissioner, n.d.[57]).

Educators and Teachers

As with parents, carers and guardians, teachers and educators hold an important role in ensuring that children can realise the benefits of the digital environment, as well as in safeguarding them against risks. Teachers may be required to help equip children with digital literacy skills, to help children respond to harmful contents or contacts they are exposed to in the digital environment, and could be asked to use digital technologies themselves in their work. Despite this, OECD research has shown that teachers consistently rate ICT skills for teaching as the second highest professional development need (after teaching students with special needs).They also report low confidence in supporting student learning through the use of digital technologies (OECD, 2018[58]).

For this reason, the Recommendation specifically highlights the need to support teachers in identifying the opportunities and benefits for children in the digital environment as well as in evaluating and mitigating against risk (at II.5.d). It further acknowledges the role that teachers play in helping children to become responsible participants in the digital environment, and that teachers require support in that role (at II.5.e). It also makes clear that educational bodies are an important stakeholder and that they should be included in any multi-stakeholder dialogue regarding the needs of children in the digital environment (at II.5.a).

Key Concepts representing critical areas for policy action

Whilst a number of factors are relevant in ensuring a safe and beneficial digital environment for children, throughout the process of developing the Recommendation, three particular issues were particularly prominent. These are: *i)* how to achieve age appropriate child safety by design, and what is meant by this concept; *ii)* the vital role of safeguarding children's privacy and personal data; and *iii)* the essential role of digital literacy.

Age Appropriate Child Safety by Design

Central to the Recommendation is the concept that both governments and DSPs should take an ageappropriate child safety by design approach in their policies and practices. For governments, the Recommendation describes this as:

- Fostering the research, development, and adoption of privacy protective, interoperable and user-friendly technologies that can restrict contact and access to content that is inappropriate for children, taking into account their age, maturity, and circumstances (at III.5.a); and
- Providing all stakeholders with clear information as to the trustworthiness, quality, user-friendliness, and privacy by design of such technologies (at III.5.b).

Within the Guidelines, DSPs are advised to take a child safety by design approach in designing or delivering services that are either directly intended for children, or where it is reasonably foreseeable that they will be accessed or used by children. This covers not just those services which have children as their intended audience, but those which children are using in reality. Determining whether or not it is reasonably foreseeable that a service will be accessed or used by children is likely to be a common sense test, to be applied on a case-by-case basis, and depend on the nature and content of the service, whether it has a particular appeal for children, and the ease of access.[19]

To this end, the Guidelines (at 1) state that in taking a child safety by design approach DSPs should:

- Pay due regard to providing a safe and beneficial digital environment for children through the design, development, deployment, and operation of their products and services, including through taking a safety-by-design approach to address risks;
- Take necessary steps to prevent children from accessing services and content that should not be accessible to them, and that could be detrimental to their health and well-being or undermine any of their rights. The efficacy of such measures should be continuously reviewed and improved where necessary;
- Regularly review and update practices to take into account changes to technology, changes in use, and consequent changes in risks for children; and
- Ensure that, when laws and policies require them, aged-based restrictions are in place to prevent children below certain ages accessing a service. Such restrictions should be proportionate to risk and privacy-preserving.

On the whole, an age appropriate child safety by design approach implies its adoption as a default design objective in any system architecture, product or service, and not added later, as an afterthought. It focuses on minimising risk through anticipating, assessing impact, detecting, and eliminating harms before they occur. At the same time, regulatory approaches should not be at the expense of children realising the benefits and opportunities of the digital environment.

The UK's Age Appropriate Design Code (UK Information Commissioners Office, 2020[59]), the Australian eSafety Commissioner's Safety by Design initiative (Australia, eSafety Commissioner, n.d.[57]) and the Recommendations from CNIL in France (CNIL, 2021[29]) all provide examples of how governments are seeking to put this concept into practice, as well as of the different approaches that can be taken. These three examples are highlighted in Box 6 below.

Box 6. Safety by Design Initiatives

The Age Appropriate Design Code focusses on UK companies' obligations under data protection law to protect children's data. It contains 15 standards that online services need to meet if children are likely to access their service. These standards take a risk-based approach and focus on providing default settings which can both ensure that children have the best possible access to online services, whilst minimising their data collection and use. The standards in the code include:

- Ensuring the best interests of the child is a primary consideration in the design and development of services;
- Undertaking data protection impact assessments to mitigate the risks to the rights and freedoms of children;
- Using an age appropriate application, and ensuring that the standards in the code are applied to child users. When it is not possible to verify if the user is a child the standards should be applied to all users;
- Ensuring that privacy information is transparent and provided in an age appropriate manner; and
- Using 'high privacy' settings by default, not disclosing children's data, and switching off both geolocation and profiling options by default, unless there is a compelling reason not to use these default settings, or to disclose children's data.

The Australian eSafety Commissioner's Safety by Design initiative take a more broad approach to risks in the digital environment, seeking to address risks in the digital environment holistically rather than just

privacy risks. This initiative takes a human-centric approach, which places the safety and rights of users at its core, taking into account their needs and expectations. At the core of Safety by Design are three principles that are designed to be actionable and achievable measures which digital service providers of all sizes can use. These principles are:

- *Service Provider Responsibility*: The burden of safety should never fall solely on the user, and service providers have a responsibility to respond to harms;
- *User Empowerment and Autonomy:* The dignity of users is of central importance, and there is a need to design features and functionalities that preserve fundamental consumer and human rights; and
- *Transparency and Accountability*: Hallmarks of a robust approach to safety;

Whilst these principles are not child specific, a youth consultation process was undertaken in the development of the principles, and they are supported by a vision statement for young people (Australia, eSafety Commissioner, n.d.[60]).

France's 'Eight Recommendations to Enhance the Protection of Children Online' (developed by the CNIL), include a recommendation on specific safeguards to protect the interests of the child (recommendation no. 8) (CNIL, 2021[61]). This recommendation seeks to encourage digital service providers to adopt good practices or establish a code of conduct, and to put in place specific safeguards to meet the child's best interests. These safeguards include:

- Putting in place strict default privacy settings;
- Deactivating by default any profiling system for children, particularly when the profiling is for the purposes of targeted advertising; and
- Preventing the reuse, and sharing of children's data for commercial or advertising purposes, unless it can be demonstrated that it is reused or shared for overriding reasons in the best interests of the child.

Source: UK, Information Commissioner's Office, Age Appropriate Design Code (UK Information Commissioners Office, 2020[59]); Australian eSafety Commissioner, Safety by Design Principles (Australia, eSafety Commissioner, n.d.[57]) France, Commission nationale de l'informatique et des libertés, Recommendation No. 8: Specific Safeguards to Protect the Best Interests of the Child (CNIL, 2021[61])

Safeguarding Children's Privacy

Today, risks to children's privacy are at the forefront of concerns regarding children's activities in the digital environment (Council of Europe, 2020[62]). Such activities are the focus of commercial interests, and can result in a multitude of monitoring and data collection and processing. Children can be data-generating subjects even when they themselves are not providing the information (e.g. school and hospital records, the sharing of children's personal data by peers and family). Additionally, with a growing reliance on using technology to deliver education services, accelerated by the COVID-19 pandemic, there are growing concerns regarding education data governance.

Research has shown that whilst children are aware that they may have contributed data about themselves or about others as a result of their activities in the digital environment, the extent to which they understand the consequences for their privacy will depend upon the child's own understanding of interpersonal relationships, which in turn depends on the child's age, maturity and circumstances. Children are aware of the 'data given'[20] primarily in interpersonal contexts (e.g. because they provide data themselves, or they may be aware that their family and friends do too). However, their understanding of how they contribute to the generation of inferred data[21] and of the value that such data has for businesses will, on the other hand,

be dependent upon their understanding of business models operating in commercial and institutional contexts – something that they are rarely taught about (Livingstone, Stoilova and Nandagiri, 2018[63]).

In light of the rising privacy concerns, children merit specific protection, as they may be less aware of the risks and consequences in relation to the processing of their personal data. Digital Service Providers have a responsibility to minimise data collection and use, to not disclose children's data, and to not use it in ways evidence indicates it is detrimental to their wellbeing[22].

The Recommendation reflects this prominent need to address privacy risks to children in several places, acknowledging upfront (in the preamble) that "safeguarding children's privacy and protecting children's personal data is vital for children's well-being and autonomy, and for meeting their needs in the digital environment". The Principles call on all Actors to support children in understanding their rights as data subjects, as well as the ways in which their personal data is collected, processed, shared, and used (at II.2.c). Additionally, in promoting digital literacy as an essential tool for meeting the needs of children in the digital environment, it is recommended that children be supported in understanding how their personal data is collected, disclosed, made available or otherwise used (at III.3.b.ii).

Additionally, the Guidelines for Digital Service Providers, give particular guidance regarding the responsibility of DSPs to safeguard children's privacy. In particular the Guidelines (at 3) recommend that DSPs should:

- Provide children with information on how their personal data is collected, disclosed, made available, or otherwise used, in a language that is concise, intelligible, easily accessible and set out in a clear and age appropriate language;
- Limit the collection of personal data (as well as its subsequent use or disclosure to third parties) to the fulfilment of the service provision, in a manner consistent with the child's best interests;
- Not use children's data in ways that evidence indicates is detrimental to their well-being; and
- Not allow the profiling of children or automated decision making, unless there is a compelling reason to do so and there are measures are in place to protect children from any harmful effects of profiling/automated decision making.

Two issues above that arise out of this part of the Guidelines merit further explanation. Firstly, it is worthwhile considering the risks associated with profiling or automated decision making, and what may be a 'compelling reason' to use these tools. Secondly, it is useful to consider what is meant by 'age appropriate language'.

Profiling, Automatic Decision Making, and Compelling Reasons

The OECD's Revised Typology of Risk (see Box 1) identified advanced technology risks as a cross cutting risk, which has the capacity to significantly affect children's lives in multiple ways (OECD, 2021[6]). Whilst advanced technologies (e.g. Artificial Intelligence, Internet of Things, predictive analytics,[23] biometrics) can have a number of benefits, they can also create new and/or amplify existing risks, for example by exacerbating inequalities; exclusion; discrimination; bias and affecting human agency (Hasse, 2019[64]). For example, biased algorithms have the potential of negatively impacting the rights of different groups of children by amplifying and replicating existing biases (for example social attitudes which may portray disabilities as negative) (UNICEF and Human Rights Center, 2019[65]). Likewise, the use of predictive analytics may raise ethical concerns, because predictive models rely on historical patterns, which may be inadvertently biased against certain subgroups of children (Teixeira, 2017[66]). Transparency on the way children's data is collected and processed through AI based technologies is therefore essential.

It is for this reason that the Guidelines recommend that, unless there is a compelling reason to do so and appropriate measures are in place to protect children from any harmful effects, DSPs should not allow the profiling of children or automated decision making in the absence of compelling reasons. A compelling

reason to allow such profiling may, for example, include the need to enable the activation of certain settings by default so that a service is accessible to a child with disabilities (e.g., identifying an ongoing need for subtitles) (UK Information Commissioners Office, 2020[59]).[24] In some countries, a compelling reason to allow such profiling may, for example, include the need to establish age or age-band to provide a child with appropriate protection (UK Information Commissioners Office, 2020[59]).

Age Appropriate Language in the Provision of Information

The Recommendation calls for providing information to children in a manner which is concise, intelligible, easily accessible and set out in clear and age appropriate language. This implies providing children with all relevant information about their privacy and the use of their personal data, such as who is collecting or using the personal data, the purposes and legal basis for doing so, who the personal data is being shared with, how long it will be kept for, and what the individual data protection rights are.[25]

The Irish Data Protection Commission's (draft) guidance on a child oriented approach to data processing, notes that when providing information to children, data controllers must ensure that the "vocabulary, tone and style of the language [used to convey the information] is appropriate to and resonates with children so that the child addressee of the information recognises that the message/information is being directed at them" (Irish Data Protection Commission, 2020[67]) The guidance notes that this means:

- Using plain and simple language tailored to the relevant age ranges of the intended audience, and that organisations should be open and honest regarding what they are doing with children's personal data. The information should be in an obvious and easy to find place, and should not be presented in a way that nudges or compels the user to consent (i.e. by appearing as a pop-up, or making the option to consent more visible); and
- carefully considering the age and developmental stages of the children likely to be using the particular service, and (where possible) using non-textual messages, such as cartoons, videos, images, icons or gamification. These methods can, depending on the age range of the user, be used to convey data protection information to children more effectively, as they are more likely to resonate with them than blocks of text. If it is necessary to use written communications, these should be presented in an eye catching manner, for example through using large fonts, bite sized texts, easy to read bullet lists, and brightly coloured texts.

The UK's Age Appropriate Design Code requires that information regarding privacy, terms of use, policies, and community standards, be provided in a manner which is "*concise, prominent and in clear language suited to the age of the child*". This includes providing specific 'bite-sized' explanations regarding how personal data is used (at the point that use is activated), tailoring information to the age of the child, and presenting information in a way that is likely to appeal to the age of the child accessing the service, that is in a 'child friendly way'. According to the Age Appropriate Design Code, child friendly techniques could include using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that will attract and interest children, rather than relying solely on written communications (UK Information Commissioners Office, 2020[59]). Likewise, France's 'Eight Recommendations to Enhance the Protection of Children Online' (developed by the CNIL) note that children need to be informed about their rights, and how their data will be used. The Eight Recommendations specify that this involves speaking to children in their own language in a manner that makes them want to pay attention. For example, through using clear, simple and short sentences, providing information only when it is necessary to make a decision, and using interactive tools (i.e. icons, videos or images) (CNIL, 2021[29]).

Additionally, both Age Appropriate Design Code and the CNIL's Eight Recommendations recognise the need for design techniques which can both speak to children in their own language, and ensure that the interface is neutral and that children are not nudged towards selecting certain options (i.e. providing consent to data collection and use) (CNIL, 2021[61]) (UK Information Commissioners Office, 2020[59]).

The Essential Role of Digital Literacy

Digital literacy is a vital underlying skill for children, in both ensuring their safety in the digital environment and in supporting them to realise its benefits. Digital literacy programs are likely to be most effective if they are accompanied by complementary policy actions, such as those to promote responsible usage and digital safety. Digital literacy is broader than merely equipping children with the necessary digital skills to access and operate digital technologies. Whilst such skills are important, digital literacy may cover such things as responding to harmful content or contact in the digital environment, to understanding commercial and privacy risks and how to critically assess information in the digital environment and recognise mis and dis-information. Digital literacy programs could also helpfully support children to realise the benefits of the digital environment, and support them to become responsible participants (OECD, 2020[5]) (OECD, 2021[68]).

It is also important that there is equitable access to digital literacy programs, and that all children are supported to attain digital literacy and skills. For example, as highlighted in the Legal and Policy review, a mismatch in digital literacy between different groups of children can exacerbate certain contact and conduct risks (OECD, 2020[5]). Specifically, it was highlighted that a greater level of digital literacy in the hands of a cyberbully, may help create the power imbalance which is inherent in many forms of bullying (Gorzig and Machackova, 2015[69]). Such a mismatch in digital literacy could arise out of the social and cultural background of those involved, highlighting the importance of community awareness and education initiatives which not only aim to ensure digital literacy across the board, but which take into account the individual, cultural and social background of those targeted for such initiatives (Gorzig and Machackova, 2015[69]).

Additionally, it is important that digital literacy initiatives are targeted at audiences broader than just children. As already noted above, often those persons who are entrusted with both developing children's digital literacy and safeguarding their interests in the digital environment (i.e. parents, carers, guardians, and teachers) often lack digital literacy skills themselves.

Accordingly, the Recommendation strongly acknowledges the importance of digital literacy and instructs governments to promote digital literacy as an essential tool for meeting the needs of children in the digital environment (at III.4). Digital literacy could include equipping children with an understanding of how the digital environment operates, how actions in the 'online world' can have consequences in the 'offline world', as well supporting children to become responsible participants in the digital environment (as recommended at II.5.e).

Certain aspects of particular importance are highlighted in the Recommendation as factors that should be considered in policy-making on digital literacy and skills. These include:

- Clarifying categories of digital risk according to age, maturity, and circumstances of children, together with harmonising the terminology used to inform the public (at III.4.a);
- Supporting children to understand how their personal data is collected, disclosed, made available or otherwise used (at III.4.b.i);
- Supporting children to critically consider and appraise information, and to increase their resilience in dealing with misinformation and disinformation[26] (at III.4.b.ii); and
- Supporting children to understand terms of service, how they can flag and report harmful content, and how they may seek redress for harms suffered in the digital environment (at III.4.b.iii).

Finally, governments are encouraged to regularly measure the evolution of children's digital literacy and skills (at III.4.C). The Recommendation also seeks to address imbalances that can arise out of inequitable digital literacy and skills, recommending that actors should seek to ensure that no child is more vulnerable to risk, or likely to suffer a future bias, because of (*inter alia*) a lack of digital literacy, or inappropriate digital literacy (at II.4.b.i, ii)

Already in 2017, when the OECD conducted its survey on the implementation of the 2012 version of the Recommendation many OECD countries indicated that media or digital literacy made up a part of their policy landscape. Many initiatives were aimed at providing children in schools or the community at large awareness raising and educative tools designed to increase knowledge about the risks associated with the digital environment and children, however less of a focus on highlighting the beneficial aspects of the digital environment was seen (OECD, 2020[5]) (Burns and Gottschalk, 2019[70]).

A number of different digital literacy frameworks and initiatives already exist.[27] For example, In France, the free public platform PIX.fr (developed by the French Ministries of National and Higher Education) provides a tool to allow children (and adults) to self-assess their digital skills and competencies in five areas: information and data; communication and collaboration; content creation; protection and security; and the digital environment (French Government, n.d.[71]). Certification of digital skills via the PIX platform is officially recognised by the French Government, and (as of 2021/2022) is mandatory for some high school and college students (French Government, n.d.[72]). In 2021, the Australian eSafety Commissioner released a Best Practice Framework to support a nationally consistent approach to online safety education. This Framework is accompanied by support materials including an implementation guide to help schools and program providers to design, deliver and review online safety education programs (Australia, eSafety Commissioner, n.d.[73]). Additionally, the research which formed the evidence base for the framework also informed the development of a Toolkit for Schools, which aims to create a safer digital environment for school communities and is recommended to be used in conjunction with the Framework (Australia, eSafety Commissioner, n.d.[74]).

Another initiative of note is the European Union's SKILLS project, which brings together different multi-disciplinary experts from leading international centres for research on media studies, communication sciences, youth research, psychology, pedagogy, law, educational neuroscience and sociology. This project seeks to build a knowledge base which will allow for better measurement of digital skills, develop evidence-based modelling regarding the impact of digital technology and digital skills on children's cognitive, psychological, physical and social wellbeing, and generate insightful evidence-based recommendations to promote digital skills and wellbeing (European Union, 2021[75])

References

#CovidUnder19 (2021), *Headline Findings: Across each of the UN Regions*, https://www.qub.ac.uk/research-centres/CentreforChildrensRights/CCRFilestore/Filetoupload,1008814,en.pdf. [32]

20 Minuten (2018), *20 Minuten Youth Lab*. [40]

Australia, eSafety Commissioner (2018), *State of Play - Youth kids and digital dangers*, https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf. [28]

Australia, eSafety Commissioner (n.d.), *Best Practice Framework for Online Safety Education*, https://www.esafety.gov.au/educators/best-practice-framework. [73]

Australia, eSafety Commissioner (n.d.), *Our Vision: Young People Safety and Design*. [60]

Australia, eSafety Commissioner (n.d.), *Safety by Design*. [57]

Australia, eSafety Commissioner (n.d.), *Toolkit for Schools*, https://www.esafety.gov.au/educators/toolkit-schools. [74]

Australian Government (n.d.), *eSafety Commissioner: About us*. [23]

Better Internet For Kids (n.d.), *Youth Pledge for a Better Internet*. [37]

BIK Youth (n.d.), *BIK Youth*, https://www.bikyouth.eu/en-GB/. [36]

Burns, T. and F. Gottschalk (2020), *Education in the Digital Age: Healthy and Happy Children*, https://www.oecd.org/education/education-in-the-digital-age-1209166a-en.htm. [15]

Burns, T. and F. Gottschalk (eds.) (2019), *Educating 21st Century Children: Emotional Well-being in the Digital Age*, Educational Research and Innovation, OECD Publishing, Paris, https://doi.org/10.1787/b7f33425-en. [70]

Byrne, J. and P. Burton (2017), "Children as Internet Users: How can evidence better inform policy debate", *Journal of Cyber Policy*, Vol. 2/1, pp. 9-52. [24]

Byrne, J., D. Kardefelt-Winther and S. Livingstone (2016), *Global Kids Online Research Synthesis, 2015-2016*, UNICEF Office of Research Innocenti and London School of Economics and Political Science, https://www.unicef-irc.org/pu. [55]

CNIL (2021), *CNIL publishes 8 recommendations to enhance the protection of children online*, https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online. [29]

CNIL (2021), *Droits numériques des mineurs : la CNIL publie les résultats du sondage et de la consultation publique*. [30]

CNIL (2021), *Recommandation 8 : prévoir des garanties spécifiques pour protéger l'intérêt de l'enfant*, https://www.cnil.fr/fr/recommandation-8-prevoir-des-garanties-specifiques-pour-proteger-linteret-de-lenfant. [61]

CNIL (n.d.), *Donées & Desing par LINC CNIL: Case Studies*. [31]

Committee on the Rights of the Child (2009), *General Comment no. 12 on the right of the child to be heard (CRC/C/GC/12)*, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGC%2F12&Lang=en. [26]

Common Sense (2017), *The Common Sense Census: Media Use by Kids Age Zero to Eight*, https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_zerotoeight_fullreport_release_2.pdf. [18]

Cortesi, S., A. Hasse and U. Gasser (2021), "Youth Participation in a digital world: Designing and implementing spaces, programs and methodologies", https://cyber.harvard.edu/publication/2021/youth-participation-in-a-digital-world. [25]

Council of Europe (2020), *Children's Data Protection in an Education setting*, https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b. [53]

Council of Europe (2020), *Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Convention 108: Children's Data Protection in an Education Setting*, https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b. [62]

Council of Europe (2017), *It's Our World: Children's Views on How to Protect Their Rights in the Digital Environment*, https://edoc.coe.int/en/children-and-the-internet/8013-it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-digital-envi. [39]

Digital Futures Commission (2021), *Child Rights Impact Assessment: a tool to realise children's rights in the digital environment*, https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf. [45]

European Commission (2021), *How to make Europe's Digital Decade Fit for Children and Young People: A Report from the Consultation with Children and Young People*, https://www.betterinternetforkids.eu/documents/167024/6847388/How+to+make+Europe%25E209s+Digital+Decade+fit+for+children+and+young+people+-+A+report+from+the+consultation+with+children+and+young+people+-+October+2021.pdf/ae344db2-5b56-0f67-625e-a66244aa02. [35]

European Commission (2020), *How families handled emergency remote schooling during the COVID-19 lockdown in spring 2020*, https://doi.org/file:///C:/Users/Robinson_L/Downloads/remote_schooling_families_summary.pdf . [78]

European Union (2021), *ySkills: A fresh approach for digital skills testing*, https://yskills.eu/. [75]

French Government (n.d.), *PIX: Cultivez vos compétences numériques*, https://pix.fr/. [71]

French Government (n.d.), *Pix: Enseignement scolaire*, https://support.pix.org/fr/support/solutions/articles/15000029308-comment-s-organise-la-certification-en-%C3%A9tablissement-scolaire-. [72]

Gorzig, A. and H. Machackova (2015), *Cyberbullying from a socio-ecological perspective: A contemporary synthesis of findings from EU Kids Online*, https://www.lse.ac.uk/media-and-communications/assets/documents/research/working-paper-series/EWP36.pdf. [69]

Hasse, A. (2019), *Youth and Artificial Intelligence: Where We Stand,, Youth and Media, Berkman Klein Center for Internet*, https://cyber.harvard.edu/publication/2019/youth-and-artificial-intelligence/where-we-stand. [64]

Hye Jung Han (2020), *As Schools Close Over Coronavirus, Protect Kids' Privacy in Online Learning*, https://www.hrw.org/news/2020/03/27/schools-close-over-coronavirus-protect-kids-privacy-online-learning. [50]

ICDPPC (2018), *Resolution on e-learning platforms*, http://globalprivacyassembly.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf. [54]

International Conference of Privacy and Data Protection Commissioners (2016), *Personal Data Protection Competency Framework for School Students*, http://globalprivacyassembly.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf. [77]

Irish Data Protection Commission (2020), *Fundamentals for a Child Oriented Approach to Data Processing (Draft version for public consultation)*, https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20App. [67]

Joint Research Centre (2018), *Young children (0-8) and digital technology: A qualitative study across Europe*, https://op.europa.eu/en/publication-detail/-/publication/9c015955-b0c5-11e8-99ee-01aa75ed71a1/language-en. [16]

Livingstone, S., M. Stoilova and R. Nandagiri (2018), *Conceptualising privacy online: what do, and what should, children understand?*, https://blogs.lse.ac.uk/medialse/2018/09/07/conceptualising-privacy-online-what-do-and-what-should-children-understand/. [63]

Livingstone, S., M. Stoilova and R. Nandagiri (2019), *Children's data and privacy online: growing up in a digital age*, https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review.pdf. [51]

Mukherjee, S. and S. Livingstone (2020), *Children and Young Peoples Voices: Digital Futures Commission*, https://digitalfuturescommission.org.uk/wp-content/uploads/2020/10/Children-and-Young-Peoples-Voices.pdf. [38]

O'Neill, B., S. Dreyer and T. Dinh (2020), *The Third Better Internet for Kids Policy Map: Implementing the European Union Strategy for a Better Internet for Children in European Union Member States*, https://www.betterinternetforkids.eu/documents/167024/26. [56]

OECD (2021), *21st-Century Readers: Developing Literacy Skills in a Digital World*, PISA, OECD Publishing, Paris, https://doi.org/10.1787/a83d84cb-en. [68]

OECD (2021), *Bridging connectivity divides*, https://www.oecd-ilibrary.org/science-and-technology/bridging-connectivity-divides_e38f5db7-en. [13]

OECD (2021), *Children in the Digital Environment: Guidelines for Digital Service Providers*, https://www.oecd.org/mcm/OECD%20Guidelines%20for%20Digital%20Service%20Providers.pdf. [7]

OECD (2021), *Guidelines for Digital Service Prividers*, https://legalinstruments.oecd.org/api/download/?uri=/private/temp/cecf7c1a-2590-4aaf-98d7-2a5f74290b92.pdf&name=Guidelines%20for%20Digital%20Service%20Providers.pdf. [81]

OECD (2021), *OECD Youthwise*. [42]

OECD (2021), *Recommendation of the Council on Children in the Digital Environment*, OECD Publishing, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [1]

OECD (2021), *Revised Typology of Risks*, https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1639766683&id=id&accname=guest&checksum=593B248065CD22CB37FA34DF785B3ECC. [6]

OECD (2020), *Combatting COVID-19's effect on children*, https://www.oecd.org/coronavirus/policy-responses/combatting-covid-19-s-effect-on-children-2e1f3b2f/. [11]

OECD (2020), *Education responses to COVID-19: Embracing digital learning and online collaboration*, https://www.oecd.org/coronavirus/policy-responses/education-responses-to-covid-19-embracing-digital-learning-and-online-collaboration-d75eb0e8/. [49]

OECD (2020), *Learning remotely when schools close: How well are students and schools prepared? Insights from PISA*, https://www.oecd.org/coronavirus/policy-responses/learning-remotely-when-schools-close-how-well-are-students-and-schools-prepared-insights-from-pisa-3bfda1f7/. [10]

OECD (2020), "Protecting children online: An overview of recent developments in legal frameworks and policies", *OECD Digital Economy Papers*, No. 295, OECD Publishing, Paris, https://doi.org/10.1787/9e0e49a9-en. [5]

OECD (2019), *OECD - University of Zurich Expert Consultation "Protection of Children in a Connected World"*, https://one.oecd.org/document/DSTI/CDEP/SPDE(2019)3/en/pdf. [17]

OECD (2019), *PISA 2018 Results (Volume I): What Students Know and Can Do*, https://www.oecd-ilibrary.org/docserver/5f07c754-en.pdf?expires=1634719190&id=id&accname=ocid84004878&checksum=43F928BE04B28EE5411D08EE5BF7F512. [8]

OECD (2018), *Teaching and Learning International Survey: Insights and Interpretations*, https://www.oecd.org/education/talis/TALIS2018_insights_and_interpretations.pdf. [58]

OECD (2012), *Recommendation of the Council on the Protection of Children Online*, https://legalinstruments.oecd.org/api/download/?uri=/private/temp/d9c3513a-221e-41ea-975b-b5bb2fe1c424.pdf&name=OECD-LEGAL-0389%20(2012)-en.pdf. [2]

OECD (2011), *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them*, https://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children- [4]

online_5kgcjf71pl28-en.

OECD (2008), *Declaration for the Future of the Internet Economy (The Seoul Declaration)*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0366. [3]

Ofcom (2021), *Children and parents: media use and attitudes report 2020 - 2021*, https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf. [21]

Ofcom (2021), *Children's Media Use and Attitudes*, https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens. [27]

Payne, L. (2020), *ENOC SYNTHESIS REPORT: Child Rights Impact Assessment*, http://enoc.eu/wp-content/uploads/2020/12/ENOC-Synthesis-Report-on-CRIA-FV.pdf. [48]

Pew Research Center (2018), *Teens, Social Media and Technology 2018*, https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/. [20]

Schleicher, A. (2019), *PISA 2018: Insights and Interpretations*, https://www.oecd.org/pisa/PISA%202018%20Insights%20and%20Interpretations%20FINAL%20PDF.pdf. [9]

Smahel, D. et al. (2020), *EU Kids Online 2020*, http://eprints.lse.ac.uk/103294/1/EU_Kids_Online_2020_March2020.pdf. [19]

T20: Task Force 4 Digital Transformation (2021), *Digital Learning for Every Child: Closing the Gaps for an Inclusive and Prosperous Future*, https://www.t20italy.org/2021/08/25/digital-learning-for-every-child-closing-the-gaps-for-an-inclusive-and-prosperous-future/. [14]

Tages-Anzeiger Youth Lab (2021), *Stell unsere Redaktion auf den Kopf! Und gestalte die Zukunft des Journalismus aktiv mit*. [41]

Teixeira, C. (2017), *Predictive Analytics in Child Welfare: An Assessment of Current Efforts, Challenges and Opportunities*, https://aspe.hhs.gov/system/files/pdf/257841/PACWAnAssessmentCurrentEffortsCh. [66]

Terre des hommes (2021), *#CovidUnder19: An initiative to meaningfully involve children in response to the COVID-19 pandemic*, https://www.tdh.ch/en/projects/covidunder19. [33]

UK Information Commissioners Office (2020), *Age Appropriate Design Code*. [59]

UK Parliament (2021), *Digital Regulation Enquiry*. [22]

UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf. [80]

UNICEF (2021), *Adolescent Perspectives on Artificial Intelligence*, https://www.unicef.org/globalinsight/sites/unicef.org.globalinsight/files/2021-02/UNICEF_AI_AdolescentPerspectives_20210222.pdf. [34]

UNICEF (2021), *Policy Guidance on AI and Children*, https://www.unicef.org/globalinsight/media/2356/file/UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021.pdf.pdf. [79]

UNICEF (2018), *Policy guide on children and digital connectivity*, https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf. [12]

UNICEF (2013), *Children's Rights Impact Assessments: A guide for integrating children's rights into impact assessments and taking actions for children*, https://sites.unicef.org/csr/css/Children_s_Rights_in_Impact_Assessments_Web_161213.pdf. [44]

UNICEF and Human Rights Center (2019), *Artificial Intelligence and Children's Rights*, https://www.unicef.org/innovation/media/10726/file/Executive%20Summary:%20Mem. [65]

UNICEF Office of Global Insight and Policy (2021), *Rapid Analysis: Digital misinformation / disinformation and children*, https://www.unicef.org/globalinsight/media/2096/file/UNICEF-Global-Insight-Digital-Mis-Disinformation-and-Children-2021.pdf. [76]

UNICEF, Save the Children and The Global Compact (2013), *Children's Rights and Business Principles*, https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf. [47]

UNICEF et al. (2020), *COVID-19 and its implications for protecting children online*, https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf. [52]

United Nations Human Rights (2011), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf. [46]

World Economic Forum (n.d.), *Generation AI: Developing Artificial Intelligence Standards for Children*. [43]

Notes

[1] See, https://www.oecd.org/about/structure/.

[2] See, https://www.oecd.org/sti/ieconomy/.

[3] Then OECD Committee for Information, Computer and Communications Policy (ICCP) Working Party on Information Security and Privacy (WPISP).

[4] The 2012 version of the Recommendation included an instruction to the Committee for Information, Computer and Communications Policy (now the CDEP) to "review this Recommendation and its implementation and to report to Council within five years of its adoption and thereafter as appropriate". In line with this instruction, the CDEP agreed, as part of its 2016 Standard-setting Action Plan, that reviewing the implementation of the 2012 version of the Recommendation and reporting to the Council thereon was the appropriate action for the Committee to take moving forward.

[5] This survey, circulated in 2017, was responded to by 34 countries: Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

[6] Represented by Delegates to the CDEP and its Working Party on Data Governance and Privacy in the Digital Economy (DGP), an informal group of experts, the Business and Industry Advisory Committee to the OECD (BIAC), the Civil Society Information Society Advisory Council (CSISAC) and the Trade Union Advisory Committee (TUAC).

[7] See more at: https://www.oecd.org/legal/legal-instruments.htm.

[8] Respectively, the COE's 'Guidelines to respect, protect and fulfil the rights of the child in the digital environment', and the Committee on the Rights of the Child's 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment'.

[9] See, Child Online Protection (itu.int)

[10] See, GPA Resolution on Children's Digital Rights (October 2021).

[11] See for example, the COE's, Guidelines on Children's Data Protection in an Education Setting.

[12] See for example, the International Consumer Protection and Enforcement Network's (ICPEN), Best Practice Principles for Marketing Directed towards children online.

[13] For example the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, developed by the Five Eyes Alliance (Australia, Canada, New Zealand, the UK and the USA).

[14] At the national level, noting that Australia is a federated State.

[15] 'Sexting' refers to the exchange of sexually explicit or suggestive messages, images or videos, usually through social media or mobile messaging applications.

[16] This was part of a broader consultation process supporting the development of digital principles for an interinstitutional declaration between the European Commission, the European Parliament, and the Council.

[17] Represented by the Alliance to Better Protect Minors Online.

[18] For example, Canada's Media Smarts program, or Belgium's 'Click Safe' program which is aimed at both parents and teachers.

[19] See also guidance on whether or not a service is likely to be accessed by children in the UK's Age Appropriate Design Code ('Services covered by this Code').

[20] Data given refers to the data contributed by individuals (about themselves or about others), usually knowingly, though not necessarily intentionally, during their participation in the digital environment

[21] "Inferred data" refers to the data derived from analysing data traces and data given, frequently by algorithms (also referred to as 'profiling'). This can also be combined with other data sources.

[22] See also UNICEF guidance, 'The Case for Better Governance of Children's Data: A Manifesto'

[23] Predictive analytics, whilst in use for some time (e.g. for forecasting), are today could be considered an advanced technology and a subset of Artificial Intelligence, due to the use of machine learning techniques to improve predictions.

[24] See also UNICEF Policy Guidance on AI and Children.

[25] See for example Articles 13 and 14 of the EU's General Data Protection Regulation (EU) 2016/679, ('GDPR').

[26] Further guidance in this regard is provided by UNICEF in its 2021 Rapid Analysis Report on Digital misinformation / disinformation and children.

[27] For example, the International Conference of Privacy and Data Protection Commissioners (now the Global Privacy Assembly) 'Personal Data Protection Competency Framework for School Students'.

Companion Document to the OECD Recommendation on Children in the Digital Environment

The OECD Recommendation on Children in the Digital Environment provides guidance for governments and other stakeholders on putting in place policies and procedures to empower and protect children in the digital environment. The Recommendation was developed in recognition that the digital environment is a fundamental part of children's daily lives, and that strong policy frameworks are needed to both protect children from any potential harm, and to help them realise the opportunities that it can bring.

This companion document aims to assist governments and other stakeholders in implementing the Recommendation. It expands upon the context in which the Recommendation was developed, and considers in detail specific aspects of the Recommendation, in particular different stakeholders and their roles (e.g. parents, governments, digital service providers) as well as key underlying concepts such as children's privacy, digital literacy and child safety by design.