Handbook for policy makers on the rights of the child in the digital environment

www.coe.int/children

Building a Europe
for and with children

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Handbook for policy makers on the rights of the child in the digital environment

to support the implementation of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe on Guidelines to respect, protect and fulfil the rights of the child in the digital environment

Handbook prepared by:
Sonia Livingstone
Eva Lievens
John Carr

Council of Europe

French edition:
Manuel pour les décideurs politiques sur les droits de l'enfant dans l'environnement numérique

All requests concerning the reproduction or translation of all or part of this document should be addressed to the Directorate of Communication (F-67075 Strasbourg Cedex or publishing@coe.int). All other correspondence concerning this document should be addressed to Directorate General of Democracy

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Photo: © Shutterstock

© Council of Europe, November 2020
Printed at the Council of Europe

The handbook has been prepared by the following authors, in close collaboration with the Secretariat of the Council of Europe Children's Rights Division:

Sonia Livingstone, Professor of Social Psychology, Department of Media and Communications, London School of Economics and Political Science (LSE), United Kingdom

Eva Lievens, Professor of Law & Technology, Ghent University, Belgium

John Carr, International Advisor on children's internet safety and security, United Kingdom

During the preparation, comments have been kindly provided by:

Laura Ferola, Official at the Italian Data Protection Authority, Rome, Italy

Professor Cristiana Carletti, Professor of International Public Law, Roma Tre University, Rome – Italy

The Belgian delegation on the Council of Europe Ad hoc Committee for the Rights of the Child (CAHENF (2019))

Contents

FOREWORD 5

A QUICK GUIDE TO RECOMMENDATION CM/REC(2018)7 FOR POLICY MAKERS 7

CHAPTER 1 – INTRODUCING THE RECOMMENDATION AND GUIDELINES 9

1. What is this handbook about? 9
2. Why was a Recommendation needed? 9
3. What is a Recommendation by the Council of Europe and how is it prepared? 10
4. How does the Recommendation relate to international and European legal standards? 10
5. What is the aim of this handbook? 11
6. Explaining key terms 12
7. Which information and communication technologies are relevant to children's rights? 13
8. What do children say? 14
9. What does the evidence show? 15
10. How is this handbook organised? 16

CHAPTER 2 – NATIONAL FRAMEWORKS 19

1. Legal frameworks 19
2. Policy and institutional frameworks 22
3. Cooperation and coordination at national level 27
4. Fundamental principles 30

CHAPTER 3 – OPERATIONAL PRINCIPLES IN PRACTICE 37

1. Access to the digital environment 37
2. Right to freedom of expression and information 40
3. Participation, right to engage in play and right to assembly and association 43
4. Privacy and data protection 45
5. Right to education 53
6. Right to protection and safety 56
7. Remedies 62

CHAPTER 4 – INTERNATIONAL COOPERATION AND COORDINATION 65

1. Ratification and implementation of UN/CoE Conventions 65
2. Cooperation with other States 66
3. Cooperation with the Council of Europe 66
4. Cooperation with intergovernmental bodies, transnational networks and other international organisations 67

CHAPTER 5 – ENGAGING WITH BUSINESS ENTERPRISES 69

IN FOCUS: ADVANCES IN ARTIFICIAL INTELLIGENCE (AI) AND IMPLICATIONS FOR CHILDREN'S RIGHTS 75

Foreword

Since their adoption by the Committee of Ministers of the Council of Europe in 2018, the "Guidelines to respect, protect and fulfil the rights of the child in the digital environment" have been praised as one of the most comprehensive sets of standards and guidance in this area. The Guidelines balance the protection of children in the digital world with the promotion of their positive rights as end users of digital technologies in their own right.

Given the increasingly important role that modern information and communication technologies play in a child's life, measures are needed to secure equal and safe access to them. If smartly used, digital technologies present enormous opportunities and benefits for children's education, leisure, access to information and participation in decisions affecting them.

This handbook is meant to support policy makers dealing with the rights of the child in the digital environment. It fosters a balanced view and approach in making political or strategic decisions in respect of the home, school or in the public sphere. Two years after the adoption of the Guidelines, the handbook aims at upholding the strong messages and guidance promoted by them and at providing all stakeholders concerned with tools and checklists to verify that no major aspect has been or will be neglected in legislative and policy making processes.

Complementing the Guidelines published in 2018, and their child-friendly version "Learn about your rights in the digital environment", published in May 2020, the handbook underlines the importance for all public bodies, civil society and private stakeholders to adopt a common approach. Whether promoted through national legislation or strategic partnerships, the well-being of children in the digital environment needs to become an objective to be jointly pursued by all stakeholders in the 21st century.

Today's children and young people are digital citizens more than any generation before them, and whilst no one is born as a "digital native", all children and young people must be supported in becoming "digitally wise". This is why the rights of the child in the digital environment is a pillar theme of the Council of Europe Strategy for the Rights of the Child (2016-2021) and it will remain a major objective in the new Strategy (2022-2027), currently under preparation by the Council of Europe Steering Committee for the Rights of the Child (CDENF).

This handbook has benefitted from inputs from many experts and organisations and will help decision-makers from a variety of backgrounds to create a digital world that truly respects, protects and fulfils the rights of the child in the digital environment.

One of the main challenges in this area is that technology is constantly evolving. As legislation and policies struggle to match its pace, the best strategy is, on the one hand, to embed the rights of the child in the development of technology and its application and, on the other hand, have developments constantly under review to be able to respond to emerging challenges. With this in mind, the handbook also tackles issues which have gained in significance since the adoption of the Guidelines, such as artificial intelligence.

I hope that this handbook will become an everyday tool for all those working in this area or whose decisions affect children in the digital environment. The recent Covid-19 crisis has reminded us of the significance of digital technologies in children's lives. At the same time, the crisis has revealed and exacerbated inequalities which cannot be ignored.

All children have a legal right to protection, participation and provision of services and it is our collective responsibility to make those rights real in every environment, including digital!

Snežana Samardžić-Marković
Director General of Democracy

A quick guide to Recommendation CM/Rec(2018)7 for policy makers

It is important for member States of the Council of Europe to establish a comprehensive, strategic national framework to coordinate, evaluate and implement policy

The digital environment is cross-cutting in its implications for children's rights. A range of public bodies and agencies will have responsibility for different areas of policy which directly impact on children's rights and the digital environment. It is essential to designate an authority or create a coordinating mechanism to ensure that these are effectively co-ordinated and are mutually reinforcing, and that the State directly engages with all relevant public and private stakeholders.

To guide States, including regional and local authorities, the following principles and rights (partly laid down in the UN Convention on the Rights of the Child) apply to all sections of the Guidelines:

- All actions and decisions must be guided by what is in the best interests of the child;
- All actions and decisions must have regard to the evolving capacities of the child;
- All actions and decisions should ensure there is no discrimination against the child;
- Children have a right to be heard on matters affecting themselves.

Six vital operational principles help to organise State-led efforts to respect, protect and fulfil the rights of the child in the digital environment

- Access to digital technology is needed to enable the exercise of a child's full range of rights, and in particular, for a child's education, inclusion and development;
- Freedom of expression includes the child's right to create and publish, and to access a diverse range of information;
- Freedom of association and assembly, along with the right to play, is vital to how children learn and develop citizenship and exercise other fundamental rights;
- Children's privacy, including their personal data, must be protected to safeguard their short- and long-term interests and development;
- The right to education today includes digital literacy, and to opportunities and resources to learn in the digital environment;
- The right to protection and safety in the digital environment underpins all children's rights, since the risk of harm in the digital environment has real consequences for a child's wellbeing.

Provision and remedies should be made available to children as rights-holders, as part of the responsibilities of duty-bearers including the State, business and other relevant actors

To implement the six operational principles in practice, a range of remedies should be developed to address the conditions under which a child's rights are jeopardised or infringed in the digital environment. Some potential infringements are best addressed by preventive actions – these may include safety and privacy-by design being incorporated into information society services and devices, and by education. Others will be responsive – crucial is ensuring child-friendly and accessible mechanisms of redress. Whilst being mindful of the precautionary principle, wherever possible measures should be evidence-based, and informed by direct consultation with children.

It is important to cooperate with major international institutions and business enterprises

The digital environment is networked and global, even though its manifestations may be different in each country and context. Effective action to ensure children's rights requires significant effort from States, international organisations as well as business enterprises. Cross-national, cross-sectoral and international cooperation will both strengthen the resources within States and bring added value internationally.

Chapter 1

Introducing the Recommendation and Guidelines

1. What is this handbook about?

In July 2018 the Committee of Ministers of the Council of Europe adopted its **Recommendation CM/Rec(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment** *("the Recommendation" henceforth)*. This document includes the world's first comprehensive guidelines for States regarding children's rights in the digital environment.

The Recommendation is an important outcome of the Council of Europe's ***Strategy for the Rights of the Child (2016-21)***. As the Strategy observes: "The digital world offers children boundless learning and connectivity opportunities as well as challenges of real concern which must be tackled by member States in an integrated manner and in line with the Council of Europe Internet Governance Strategy 2016-2019. The Council of Europe will provide guidance and support to member States in ensuring children's participation, protection and provision rights in the digital environment."[1] On this basis, this handbook provides guidance and support to policy makers of various backgrounds.

2. Why was a Recommendation needed?

The digital environment is complex and can be subject to rapid and sometime unpredictable change. It is reshaping children's lives in many ways, resulting in opportunities for and risks to their well-being and enjoyment of human rights.[2] In the preamble to the Recommendation, the Council of Europe recognises that information and communication technologies (ICTs) are an important tool in children's lives for education, socialisation, expression, inclusion and development, while their use can generate risks, including violence, exploitation and abuse.[3]

1. Council of Europe Strategy on the Rights of the Child 2016-2021, p. 20.
2. Preamble.
3. Preamble.

The Recommendation includes comprehensive guidelines which specify how States can ensure that children receive the support and guidance that they are entitled to in their discovery and use of the digital environment, respecting their rights and dignity. The guidelines recognise that children of all ages (up to the age of 18) are affected by the ways in which other people and institutions use ICTs. The guidelines encompass the obligations for States and the responsibilities of other stakeholders, including international, national, regional, local institutions and businesses.

3. What is a Recommendation by the Council of Europe and how is it prepared?

Recommendation CM/Rec(2018)7 was adopted by the Committee of Ministers, the Council of Europe's main decision-making body. A Recommendation is not binding on the 47 member States of the Council of Europe, but it provides a framework and proposals that governments should implement at the national level. It is the outcome of a formal and comprehensive deliberative process in which all member States were involved. It resulted in a consensus and a commitment to implement the Recommendation.

The substantive text of the Recommendation was prepared by the Ad Hoc Committee on the Rights of the Child (CAHENF) and the Drafting Group of Specialists on Children and the Digital Environment (CAHENF-IT). During this process international organisations and businesses were consulted. Also, importantly, children in seven countries across Europe were directly consulted as were children's rights and welfare organisations, to reflect and represent children's concerns. Follow-up of the Recommendation is ensured by the Steering Committee for the Rights of the Child (CDENF).

4. How does the Recommendation relate to international and European legal standards?

The Recommendation reaffirms the commitment of member States to ensure that every child enjoys the full range of human rights enshrined respectively in the United Nations Convention on the Rights of the Child (UNCRC), in the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), and their relevant protocols.[4]

It also has regard to obligations and commitments expressed in other relevant international and European conventions, such as, at Council of Europe level, the revised European Social Charter (ETS No. 163), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), the Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), the Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197), the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), the Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210).

4. Preamble.

In other words, while the Recommendation is not itself binding, many of its provisions rely on or reflect already binding legal Conventions of the Council of Europe. Many, too, are based in national laws and regulations, depending on the State. Finally, the Recommendation takes into account resolutions and declarations of the Committee of Ministers and the Parliamentary Assembly of the Council of Europe in this field.

5. What is the aim of this handbook?

This handbook aims to support Council of Europe member States, and especially legislators and other "policy makers" (including governments and parliaments at central, regional and local levels) as well as academia, human rights agencies and relevant civil society organisations in implementing Recommendation CM/Rec(2018)7 and the *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*. It is recognised that State authorities at different levels work with many other actors, including businesses and relevant international bodies, in developing policy and practice regarding children's rights in relation to the digital environment. Hence the handbook identifies other stakeholders that member States could or should engage with to implement the guidelines and it provides concrete action points for States to engage with stakeholders and help them meet their responsibilities.

The handbook is intended to be user-friendly and practical. It recognises that States may already be undertaking a range of actions and offers the "added value" of integrating in a single coherent and comprehensive document the wide array of issues to be addressed so that children's rights are respected, protected and fulfilled in this fast-evolving digital age. It explains how national frameworks and policies can be formulated, advises on how important operational principles and measures can be put in practice and highlights how international cooperation can be advanced. In each chapter, the applicable legal standards are noted. Checklists allow for a detailed assessment and evaluation of the implementation process by States.

At the heart of the Recommendation lie three main expectations of the governments of the member States, namely that they:[5]

- "review their legislation, policies and practice to ensure that they are in line with the recommendations, principles and further guidance set out in the appendix of this Recommendation, promote their implementation in all relevant areas and evaluate the effectiveness of the measures taken at regular intervals, with the participation of relevant stakeholders" (Recommendation 1)
- "require business enterprises to meet their responsibility to respect the rights of the child in the digital environment and to take implementing measures, and encourage them to co-operate with relevant State stakeholders, civil society organisations and children, taking into account relevant international and European standards and guidance" (Recommendation 3)

5. Preamble.

- "co-operate with the Council of Europe by creating, implementing and monitoring strategies and programmes that respect, protect and fulfil the rights of the child in the digital environment, and share, on a regular basis, examples of strategies, action plans, legislation and good practices related to the implementation of this Recommendation." (Recommendation 4)

In addition to guiding policy makers, this handbook aims to answer the concerns of those who fear that supporting children's rights in the digital environment is too difficult or that State action risks being ineffective, disproportionate, too quickly outdated or introducing unintended adverse consequences. It does this by offering pragmatic guidance and advice (including in form of checklists), and by pointing to the sizable body of recognised and relevant legal standards as well as a range of valuable resources for interpreting and implementing them.

6. Explaining key terms

Child

As defined in the guidelines, "a child" refers to anyone under the age of 18 years. This definition accords with UNCRC article 1. Note that while the UNCRC qualifies this for States where the age of majority is attained earlier, the usual age of majority in Council of Europe member States is 18 years,[6] notwithstanding that different States will apply various markers of maturity in the teenage years.[7]

Rights

In addressing the rights of the child in the digital environment, the Recommendation and guidelines concern fundamental human rights as noted in section 1.4. This is distinct from what are colloquially called "digital rights" (as in the "right to be forgotten" by a search engine or the "right to internet access").

In specifying the obligation of States to respect, protect and fulfil the rights of the child in the digital environment, the Recommendation draws on the language of international human rights law:[8]

> *"International human rights law lays down obligations which States are bound to respect. By becoming parties to international treaties, States assume obligations and duties under international law to respect, to protect and to fulfil human rights. The obligation to respect means that States must refrain from interfering with or curtailing the enjoyment of human rights. The obligation to protect requires States to protect individuals and groups against human rights abuses. The obligation to fulfil means that States must take positive action to facilitate the enjoyment of basic human rights."*

6. Council of Europe, Recommendation CM/Rec (2012)2 of the Committee of Ministers to member States on the participation of children and young people under the age of 18 (Adopted by the Committee of Ministers on 28 March 2012 at the 1138th meeting of the Ministers' Deputies).
7. Council of Europe, Resolution (72) 29 on the lowering of the age of full legal capacity (Adopted by the Committee of Ministers on 19 September 1972 at the 213th meeting of the Ministers' Deputies). See also FRA publication on Minimum age requirements in the EU.
8. See UN webpage on International Human Rights Law.

Digital environment

There is no simple definition of the digital environment. This is because it is increasingly broad and diverse, it continues to change and innovate, and it is manifested differently across countries and contexts. The guidelines offer a broad definition, encompassing information and communication technologies (ICTs), including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services.[9] This definition is designed to include a host of specific phenomena, including some not yet invented, and some whose names and operation may change over time. This is to future-proof the Recommendation as far as possible. The notion of 'environment' is meant to capture the extensiveness and interconnectedness of information and communication technologies as they become embedded in children's everyday lives.

7. Which information and communication technologies are relevant to children's rights?

In 2017, European homes, including homes with children, were the most internet connected in the world, although there are considerable differences and inequalities in access and use both within and across countries.[10] As the ITU comments, "There are skill inequalities between children as much as there are between adults, …available data suggest that digital inequalities are not a generational thing and will persist into the future."

Access via a computer is increasingly supplemented or even replaced by access via a smartphone. Meanwhile, connected devices ("Internet of things") are gaining popularity, including a range of smart home devices, connected toys and clothes, and other everyday objects (health appliances, domestic tools, car sensors, recording devices, etc.). Augmented and virtual reality headsets, robotics and other technological innovations are increasingly important in children's lives. Access to the internet means access to a rapidly expanding array of content and services, underpinned by a complex networked economy of third parties. These in turn rely on algorithmic processing or data analytics, artificial intelligence and transnational transactions as well as personal profiling and marketing activities. In considering which information and communication technologies are relevant to children's rights, it is important to include not only those which children use, but also those which others use – whether individuals or institutions.

Taken together, all of these uses affect the context in which children are growing up, altering the risks they face for their well-being, and the numerous opportunities open to them. For example, if a child lacks access to technologies used by most of his or her peers, if a nursery processes the personal data of the infants in its care, or if potential abusers deploy technologies of which a child is unaware, the child's rights may be infringed.

9. Guidelines, section 1.
10. Source: ITU (2018) Measuring the information society 2018. Note that the ITU's definition of 'Europe' includes 50 countries largely overlapping with Council of Europe member States.

Questions to consider:

- Which ICTs are most used by children in your country?
- What inequalities exist in the access and use of different groups of children (e.g. according to the child's age, and the child's or his or her parents' or legal guardians' race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth, or other status)?
- Which ICTs are being used in sites or services used by children (for example, nursery, school, library, medical centre)?
- Which new or emerging ICTs are on the horizon, and is there sufficient evidence available to track and assess their diffusion, adoption and likely consequences?
- Are there other ways in which the digital environment may positively or negatively impact on children's rights?

8. What do children say?

In preparing the Recommendation, the views of children were considered, in accordance with UNCRC article 12 and the Council of Europe Recommendation CM/Rec(2012)2 on the participation of children and young people under 18. Following a desktop review, eight reports (from Croatia, Cyprus, Czech Republic, Germany, Hungary, Italy, Romania, Ukraine) based on direct consultations with children regarding their rights in the digital environment were analysed.[11] As the synthesis report notes, "Despite the diverse and different backgrounds of the children …they expressed similar views and made the same recommendations in relation to several issues." Examples of children's views are:

> *"When we get older, we get smarter and have better understanding of the internet and we have better rights on the internet" (Croatia)*
>
> *"Internet access should be a common good and not a privilege." (Italy)*
>
> *"We are against discrimination by age." (Ukraine)*
>
> *"It's really important for us to have an opportunity to participate, not only in daily life, but also on the internet, especially on social sites where we stay in touch with our friends." (Czech Republic)*
>
> *"Children have a human right to play, to talk to their friends and to explore their life" (Ukraine)*

Children's concerns and recommendations, based on consultations in eight countries

- Children are unanimous that everyone should have access to the internet, and that some access should be free of charge and non-discriminatory.
- They value internet access for learning, play, socialising and expression. To support this, the most common call from children is for digital literacy education in the state curriculum.

11. Council of Europe (2017) It's our world: children's views on how to protect their rights in the digital environment.

- Children are aware of their right to play but differ in their views of what kinds of play, and how much play, is advisable online.
- Children recognise the importance of their evolving capacities, realising that they understand the digital environment better as they get older.
- Equality is of overarching importance to children, and it is especially prioritised by more vulnerable groups and those likely to experience discrimination such as those with learning disabilities, ethnic minorities and unaccompanied minors.
- Respect for private and family life was especially emphasised by vulnerable groups – with the importance of staying in touch emphasised by asylum-seeker children, for instance.
- One main concern centred on data protection and the right to privacy. Linking this to safety, children worry about how their photos might be misused, or how abuse of their personal information could lead to being hurt offline, in their 'real lives.'
- They called for child-friendly, easily understandable terms and conditions and other measures so that they can make their own decisions about engaging with websites and apps.
- Children value support and guidance from parents and caregivers, but they emphasise also the importance of balanced, and not unduly protective measures.
- While aware of online risks such as cyberbullying, grooming and hate speech, children called for more information and better sources of support, as often they do not know where to turn for help when needed.

9. What does the evidence show?

Efforts to respect, protect and fulfil the rights of the child in the digital environment must be grounded in robust and up-to-date evidence. While such evidence is not always sufficient, this handbook has been informed by the best evidence and expertise available. Although the digital environment continues to innovate and evolve, a number of research findings are proving fairly stable, offering a reasonable basis for the development of policy and practice. For example, the main five findings from the 33 country EU Kids Online network in 2014[12] were that:

1. The more children use the internet, the more digital skills they gain, and the higher they climb the 'ladder of online opportunities' to gain the benefits.
2. Not all internet use results in benefits: the chance of a child gaining the benefits depends on their age, gender and socio-economic status, on how their parents support them, and on the positive content available to them.
3. Children's use, skills and opportunities are also linked to online risks; the more of these, the more risk of harm; thus, as internet use increases, ever greater efforts are needed to prevent risk also increasing.

12. EU Kids Online Final Report (2014). These findings have since been reinforced by EU Kids Online's 2020 report.

4. Not all risk results in harm: the chance of a child being upset or harmed by online experiences depends partly on their age, gender and socio-economic status, and also on their resilience and resources to cope with what happens on the internet.
5. Also important is the role played by parents, school and peers, and by national provision for regulation, content provision, cultural values and the education system.

The challenge is that the available evidence tends to draw more on the experiences of older children in richer than poorer countries – and it is not always sufficiently up to date. However, new research continues to be conducted and the evidence base is expanding.[13]

Evidence is necessary for effective policy design and implementation because it can, among other things:

- Identify the prevalence, nature and distribution of problems
- Set a baseline and track the scale and nature of change
- Evaluate whether or not interventions are beneficial and why
- Test assumptions, and counter myths and misunderstandings
- Inform the targeting of resources by demographic, geographic or other factors
- Gather and represent the views of those insufficiently heard in public policy
- Reveal hidden experiences or differences in perspective
- Inform decision-making and provide indicators to assess the results
- Critically analyse problems and propose alternative solutions

Key organisations producing relevant research evidence include:

- European Commission's Better Internet for Kids programme
- EU Kids Online and Global Kids Online projects
- ICMEC[14]
- International Telecommunications Union (Statistics Department; Child Online Protection)
- OECD
- UNESCO
- UNICEF

13. Useful examples include Council of Europe (2016). Mapping of media literacy practices and actions in EU-28; United Nations (Ed.), *Ending the torment: tackling bullying from the schoolyard to cyberspace* (pp.115-122), New York: Office of the Special Representative of the Secretary-General on Violence against Children; UNICEF (2017). *State of the World's Children: Children in a digital world*. New York: UNICEF. Deloitte and Ipsos MORI (2019) *2nd Survey of Schools: ICT in Education*. Brussels: European Commission.
14. See, for example, Studies in Child Protection (2018).

10. How is this handbook organised?

The pillars of this handbook are as follows:

Chapter 2 sets out the importance of establishing a comprehensive and strategic national framework by which States, including national, regional and local authorities, can ensure that they respect, protect and fulfil the rights of the child in the digital environment. It accompanies and should be read in conjunction with section 4 (National frameworks) of the guidelines.

Chapter 3 provides interpretative and practical guidance for each of the operational principles which comprise the main part of the guidelines. It accompanies and should be read in conjunction with section 3 (Operational principles and measures) of the guidelines.

Chapter 4 explains the wider international context, to guide States to the key international organisations who will support their actions and with whom they should cooperate. It accompanies and should be read in conjunction with section 5 (International co-operation and co-ordination) of the guidelines.

Chapter 5 recognises that business represents crucial actors in relation to the digital environment. It brings together the responsibilities of business so as to guide States in meeting their obligations regarding children's rights in relation to the digital environment.

There are four transversal or cross-cutting themes, partly drawing on the fundamental principles of the UN Convention on the Rights of the Child, and relevant to all chapters:

- All actions and decisions must be guided by what is in the best interests of the child
- All actions and decisions must have regard to the evolving capacities of the child
- All actions and decisions should ensure there is no discrimination against the child
- Children have a right to be heard on matters which affect them

In most chapters, specific questions to be addressed by decision-makers in designing laws, policies and mechanisms which fully take children's rights into account, are included in checklists and thus very hands-on tools for decision-makers of different backgrounds.

Last, States face a range of unresolved or contentious issues. These are presented in text boxes which highlight the challenges and provide guidance or sources of further information where available.

Chapter 2

National frameworks

The Recommendation encourages member States to review **legislation**, **policies** and **practice** to ensure that the rights of the child in the digital environment are respected, protected, and fulfilled. This chapter includes guidance for implementation regarding legal frameworks and national policies and coordinating mechanism, and explains which fundamental, cross-cutting principles must be taken into account in all actions by States. The next chapter looks at how the operational principles and measures of the Recommendation can be put into practice.

Shaping national legal, policy and institutional frameworks requires the involvement of all levels of government. Because of the differences in national governance and administration structures, it may be challenging to identify which **ministries, agencies, departments and other administrative bodies** should be involved (2.1. and 2.2.). A first step in the implementation of the Recommendation is to designate an authority or create a coordinating mechanism following a transversal approach (e.g. the Ministries of Education or Family (by starting from line ministries), or Ministries of Media or the Digital Agenda (by taking a broader view), data protection authorities, or the Ombudsperson for Children, or similar). Then it is vital to map and identify relevant state bodies at national, regional and local level. **Other stakeholders** also need to be drawn into these processes (2.3.).

To respect, protect and fulfil their rights in the digital age, in some cases it will be most effective to mainstream their rights into established policy sectors for the general population,[15] ensuring that stakeholders understand why children's rights are included; in other cases, it will be more effective to develop specific actions, or establish specific organisations, to address children's rights in this new and challenging environment.

1. Legal frameworks

The Recommendation requires member States to review at regular intervals, and, where necessary, update legal frameworks to support the full realisation of the rights of the child in the digital environment. This entails, first, that States identify which laws are already in place, whether there are gaps or overlaps in the framework and which bodies are competent to enforce those laws. Furthermore, it is important to acknowledge that not everything in the digital environment can or should be regulated by means of (traditional) legislation. Voluntary measures by private actors or measures that are underpinned by cooperation between public and private actors may also play a role.[16] States should require business enterprises to perform regular child-rights risk assessments (also called child rights impact assessments) before their digital products or services could reach or affect children.

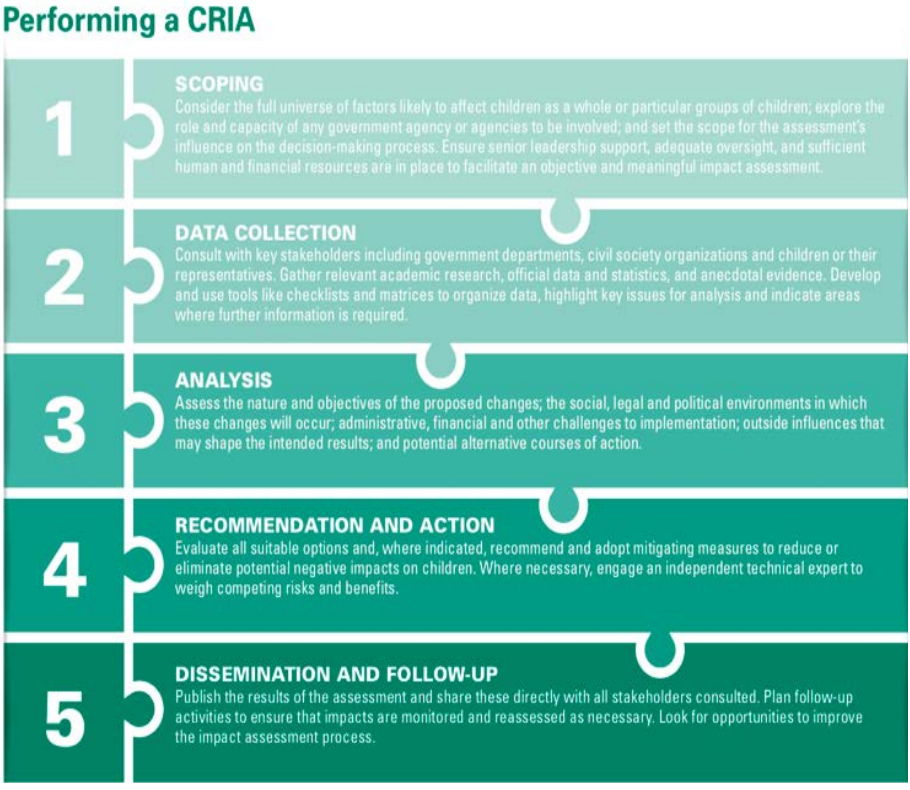
15. See European Commission "Introduction to Child Rigths Mainstreaming".
16. Preamble: "Conscious that policies in this area require a combination of public and private, legal and voluntary measures, that all relevant public and private stakeholders share responsibility for ensuring the rights of the child in the digital environment, and that co-ordination of their actions is necessary"

Questions / checklist for member States

- Which laws are in place that are relevant to realise (i.e. protect and fulfil) the rights of the child in the digital environment? Are there gaps and weaknesses in the current legal framework? Which are the competent bodies that enforce the existing laws?
- Are there child rights impact assessment (CRIA) processes in place to evaluate (new) laws and policies that are (going to be) adopted and that relate to the digital environment?[17]

Steps required for the performance of a Child Rights Impact Assessment[18]

Five steps for the performance of a Child Rights Impact Assessment



17. For example, see: FRA webpage on "Child Rights Impact Assessment";
18. Source: *United Nations Children's Fund (UNICEF) and International Commission of Jurists (ICJ)* (2015) Obligations and Actions on Children's Rights and Business: A practical guide for States on how to implement the United Nations Committee on the Rights of the Child's General Comment No. 16.

Questions / checklist for member States

- Is there a national mechanism that ensures periodical review and updates of the legal framework to support the full realisation of the rights of the child in the digital environment?
- Does your national legal framework:
  - provide for preventive and protective measures in relation to the digital environment?
  - promote positive services (i.e. content and services that enhance children's well-being promoted through goals for educational curricula, programmes of public broadcasters or funding for innovative media content)?
  - provide support measures for parents and caregivers?
  - prohibit all forms of violence, exploitation and abuse?
  - include effective remedies, and easily accessible recovery and reintegration services?
  - establish child and gender-sensitive counselling, reporting and complaint mechanisms?
  - encompass child-friendly mechanisms for consultation and participation?
  - set up accountability mechanisms to fight impunity by closing loopholes or gaps?
  - foresee educational measures for children who do not respect the rights of their peers in the digital environment?
- Is there a legal framework in place that aims to address the full range of unlawful acts that can be committed in the digital environment, formulated in a technology-neutral manner? Does this legal framework include definitions of offences, criminal, civil or administrative liability and sanctions for natural and legal persons and provisions of services for children?
- Does your national legal framework prevent the criminalisation of children when it comes to violence committed by children, including peer-to-peer online violence or abuse? Are preventive and restorative approaches (including educational measures) adopted in relation to such situations?
- Are the following instruments ratified and implemented?
  - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201)?
  - Council of Europe Convention on Cybercrime (ETS No. 185)?
  - Optional Protocol to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000)?[19]
  - Optional Protocol to the United Nations Convention on the Rights of the Child on a communications procedure (2011)?
- Is there a national data protection law in place that applies to the processing of personal data of children? Is this law in conformity with the Modernised Convention 108?

19. See the UN Committee on the Rights of the Child's (2019) guidelines on implementing the Optional Protocol.

- Is there a national independent data protection authority that is competent to handle complaints by children and/or their legal representatives and to establish effective and easily accessible mechanisms that enable children to exercise their data subject rights?
- Does the national legal framework in place provide for a predictable regulatory environment that helps businesses and other stakeholders meet their responsibility to respect the rights of the child in the digital environment throughout their operations?
- Does the national legal framework allow for children and/or their legal representatives to seek compensation for violations of their rights and abuse? Is there a fund that compensates child victims? Are measures in place that provide therapeutic or other support?
- Does the national legal framework include a requirement for entities that want to become the registry for a generic or country code top-level domain to have due regard to the best interests of children? Is there a requirement in the national legal framework that prohibits the registration or use of any domain name which advertises or suggests that child sexual abuse material may be available on any domain?
- Does the national legal framework require registrants wishing to establish or renew a site or service targeted at children or used by children in substantial numbers (within a generic or country code domain) to put in place appropriate child protection policies?

2. Policy and institutional frameworks

Comprehensive national strategic approaches are useful to ensure that policies and measures are consistent and mutually reinforcing in leading to greater co-ordination and policy coherence. This can be achieved through stakeholder engagement, informed sectoral policies, child-risk assessments, and child-sensitive institutions and mechanisms of all kinds (awareness-raising, campaigning, consultation and participation, counselling, reporting and complaint etc.). Sufficient investment and resources and adequate trainings of professionals are key to effectively implement policy and institutional frameworks.

Questions / checklists for member States

Overall strategy and policy coherence

- Is there a **comprehensive strategic national approach** to ensure that the rights of the child in the digital environment are respected, protected, and fulfilled? Is there either a strategy or action plan dedicated to children's rights in the digital environment or a mechanism to ensure the integration of specific attention to the rights of the child in the digital environment into existing action plans, strategies and policies in a consolidated manner?
- Does the comprehensive strategic national approach:
  - identify competent bodies with the responsibility and authority to implement the actions (including designating an authority or creating a coordinating

mechanism to take the lead in advancing and coordinating actions regarding children's rights in the digital environment)?

- contain realistic and time-specific targets?
- provide for sufficient support by making available adequate human and financial resources?
- take into account current scientific knowledge, based on ongoing and sufficiently resourced research and good practices?
- provide for means and measures to inform children about their rights and the existing remedies?
- provides for actions and campaigns to create awareness on children about the consequences deriving from the violation of others' rights?

- Are / were relevant stakeholders engaged in the design, drafting, implementation and evaluation of a national strategy or action plan?

Relevant stakeholders include:

- specialised ministries (e.g. children, youth, family, social affairs, media, justice, digital agenda, innovation, care/welfare etc.)
- ombudspersons for children
- other independent human rights institutions
- specialised digital, media and information literacy organisations
- education stakeholders, including information and counselling organisations for youth
- data protection authorities
- business enterprises
- civil society, including child and youth-led organisations
- networks
- specialists
- coordination organisms

- Have children been:
  - informed about their rights in the digital environment and existing remedies?
  - consulted and empowered to contribute to the preparation of national policy and institutional frameworks, with their informed consent and according to their evolving capacities?
  - informed about how their views were taken into account and how these views influenced the decision-making process?
  - involved through meaningful participation processes, thanks to adequate resources being made available ?
  - involved through child participation processes embedded in child safeguarding policies?

Children are stakeholders, too

Do you know about and have you made use of the Council of Europe's Child Participation Assessment Tool (CPAT) providing for self-assessment indicators for national child participation mechanisms and practice?

- Is there a methodology in place to assess progress and evaluate actions foreseen by the national strategy or action plan at all levels and by all stakeholders (including coordinated templates ready for use)?
- Are regular evaluations conducted with a view to identifying policies and measures that are appropriate and effective in respecting, protecting and fulfilling the rights of the child in the digital environment?
- Is information on adopted strategies or action plans and their implementation widely disseminated?

Sectoral policies

- Are policies and initiatives informed by rigorous and up-to-date evidence about children's experiences in the digital environment, in order to map existing opportunities and risks for children (according to different age groups), identify emerging trends and guide the targeting of policy and resources to ensure children's well-being in the digital environment?
- Are there policies in place that support educational, cultural, public broadcasters and other institutional providers of beneficial resources for children to make these available to children, parents and caregivers in the digital environment?
- Are regulatory agencies held responsible for drawing up, implementing and enforcing standards and guidance relevant to the rights of the child in the digital environment?
- Are measures taken (e.g., policies, operational guidelines and/or codes of conduct), to build awareness and support among business enterprises within their jurisdiction regarding their roles, responsibilities and impact on the rights of the child, and their co-operation with relevant stakeholders?
- Are measures and actions targeted according to children of different age ranges?
- Within the national framework for child protection, is a comprehensive protection and safety policy drawn up within which the digital environment is expressly addressed? Have all relevant stakeholders including children, contributed to such a policy? Does the policy take into account existing standards and guidance, such as the Council of Europe *Policy Guidelines on integrated national strategies for the protection of children from violence* (2009)?
- Are there strategies in place to prevent citizens' access to child sexual abuse material hosted in other jurisdictions?
- Are business enterprises and other relevant stakeholders engaged in the implementation of sectoral policies?
- Is there a digital and media literacy policy in place that provides children and their caregivers with access, creative opportunities, critical awareness and reflection on their conduct?

Addressing the risks and impact for the rights of the child

- How do you require business enterprises and other stakeholders to undertake **due diligence** in order to identify, prevent, mitigate their negative impact and maximise their positive impact on the rights of the child in the digital environment?
- How do you require business enterprises to perform regular child-rights risk assessments in relation to digital technologies, products, services and policies and to demonstrate that they are taking reasonable and proportionate measures to manage and mitigate such risks?
- How do you encourage business enterprises to develop, apply and regularly review and evaluate child-oriented industry policies, standards and codes of conduct to maximise opportunities and address risks in the digital environment?
- How do you require business enterprises to take reasonable, proportionate and effective measures to ensure that their terms and conditions of service are enforced and comply with national legislation?

Institutional aspects, mechanisms and services

- Do institutions responsible for guaranteeing human and children's rights address within their mandate the rights of the child in relation to the digital environment? Examples of such organisations are:
  - ombudspersons for children/children's rights commissioners
  - independent human rights institutions
  - data protection authorities
  - media and communication regulators
- Are there institutions or bodies that are competent to receive, investigate and address complaints from children and their parents or legal representatives about human rights violations or abuses in relation to the digital environment? Do these institutions or bodies employ child-sensitive procedures that ensure the child's right to privacy throughout and provide for monitoring and follow-up?
- Are accessible, safe, confidential, age-appropriate and gender-sensitive counselling, reporting and complaint mechanisms in place? Examples are:
  - hotlines for reporting and take down of child sexual abuse material
  - helplines for children (and the public)
  - zero-rated chat applications managed by child helplines
  - online platforms, with appropriate links to child support services and law-enforcement authorities, and, where appropriate, in close co-operation with external stakeholders
  - safe, child-friendly, free-of-charge points of contact and procedures for children to report violence, exploitation and abuse in the digital environment to the relevant authorities.

- Are telecommunications companies encouraged to waive costs for calls to and from child helplines?
- Is there an effective mechanism in place to allow any person to report anonymously the existence of suspected illegal material online, in particular child sexual abuse material?
- Is access ensured to adequate and gender-sensitive support services and is assistance provided for children whose rights and privacy have been violated, for example by violence, sexual exploitation or abuse in the digital environment, including where sexual images have been produced and distributed? Are there services and mechanisms in place to ensure the child's physical and psychological recovery and social reintegration, and prevent their re-victimisation?
- Are sex-offender treatment programmes available for persons convicted of sexual offences involving children in the digital environment? Are therapeutic services available to anyone concerned about the possibility of their committing a sexual crime involving a child, including in the digital environment?
- Are there any distinctive programmes or services available for young offenders, and on violence or harmful sexual behaviour committed by children or amongst peers ("peer violence")?

Investment, resources and training

- Does the state invest in ICT hardware, software, connectivity, adequate bandwidth and teacher training in schools to support learning?
- Does initial and in-service training inform and empower educators so that they can support children in acquiring the skills and literacy needed to exercise their rights in the digital environment?
- Are there policies and measures in place that provide educational institutions with the resources, training and support needed to take preventive and protective measures concerning children, including in school, against violence and abuses of digital media, in ways that prevent escalation, provide appropriate support to children affected by and involved in such acts, provide redress and build resilience?
- Are there measures that ensure that adequate arrangements are in place to implement screening processes and to provide guidance, advice and assistance to any agency or employer who recruits staff or volunteers to work with children, including within the digital environment, in order to prevent and reduce the risk of individuals with a criminal record being recruited or placed in a position of trust vis-à-vis children?
- Are adequate resources allocated to and is initial and continuous training provided for law-enforcement staff, members of the judiciary and professionals working with and for children at national, regional and local levels? Such training should enhance their skills and knowledge of the rights of the child in the digital environment, the risks children face online, how to recognise the signals that a child may be a victim of online harm, violence, abuse and exploitation (both by adults or other children) and what steps to take in response.

- Is there investment in research and knowledge development, including child and youth participation in the field of the rights of the child in the digital environment? Is research being conducted independently of relevant interests and sufficiently detailed to differentiate children's experiences by age, sex, socio-economic status and other factors that render children vulnerable or resilient in the digital environment? Does the state invest in ICT hardware, software, connectivity, adequate bandwidth and training of trainers in care institutions for children with a disability or who are placed out of the home due to harmful family circumstances or delinquent behaviour, or who are unaccompanied refugee minors?
- Does initial and in-service training for youth care professionals inform and empower them so that they can support children in acquiring the skills and literacy needed to exercise their rights in the digital environment?

Example of good practice – The Flag System for the prevention of sexual aggression[20]

The Flag System is used for the prevention of sexual aggression and in supporting healthy sexual development: making sexuality, desires, boundaries, criteria and gradations of sexual behaviour insightful and a subject of discussion, since it makes talking about sexual behaviour easier. Many professionals are uncertain about what is and what is not acceptable. The questions 'How can I help children and young people to assess when sexual behaviour is ok or not?' and 'How do I respond to (un)acceptable behaviour?' are very relevant these days. The Flag System offers an answer to these questions.

3. Cooperation and coordination at national level

Each State will need to work with a wide range of stakeholders insofar as the activities of each impact on children's rights in the digital environment. States are strongly advised to designate an authority or create a coordinating mechanism ("lead organisation").[21] The particular mix of stakeholders is likely to vary by country, so it will first be important to identify relevant stakeholder groups. Stakeholders operate at local as well as national, regional and international levels, and children's lives are often shaped by actions and provision at local level. As elaborated in section 2.4, it is vital to consult with and listen to children. Further, it is important that States recognise, support and address the role of parents, caregivers and families as stakeholders.[22]

20. For more information see Flagsystem the dedicated webpage by Rutgers and Sensoa (Netherlands).
21. As revealed in the European Commission's mapping of policy and practice for a "Better internet for kids", advances are greatly impeded by the lack of a national coordinating body. See O'Neill, B., Dinh, T. (2018). The Better Internet for Kids Policy Map: Implementing the European Strategy for a Better Internet for Children in European member States.
22. See Council of Europe Digital Parenting Guide.

The role of parents[23]

Parents and caregivers have a vital role to play in realising children's rights generally, including in the digital environment. It is of primary importance, therefore, that the state supports parents in caring for their children in relation to the digital environment, by providing information, resources and help services for parents as well as relevant training for professionals who engage with parents.

However, there are some difficulties to consider:

- Parents may (feel themselves to) lack the digital skills and knowledge needed to keep up with, and support their children and keep them safe online
- Parents can be hard to reach by the state, with parental information and awareness raising requiring expensive communication means
- Parents tend to be risk-averse, more focused on child protection than on facilitating children's rights to express themselves, meet others or play online
- Especially when anxious about the risk of harm, parents can struggle to respect a child's right to privacy
- A minority of parents represents a direct or indirect threat to children's safety and well-being

Note that relevant stakeholders will include both those whose express purposes concern children and also those whose purposes are not necessarily directly concerned with children but whose actions may impact on children, nonetheless. To ensure that all relevant stakeholders become cognisant of their responsibility regarding children, mainstreaming children's rights into existing policy for the general population will be crucial.

To ensure each stakeholder group meets its responsibilities, States should work with each to specify and support a positive direction, coordinating their actions to reinforce synergies and ensuring gaps in provision or conflicts do not arise.

Questions / checklist for member States

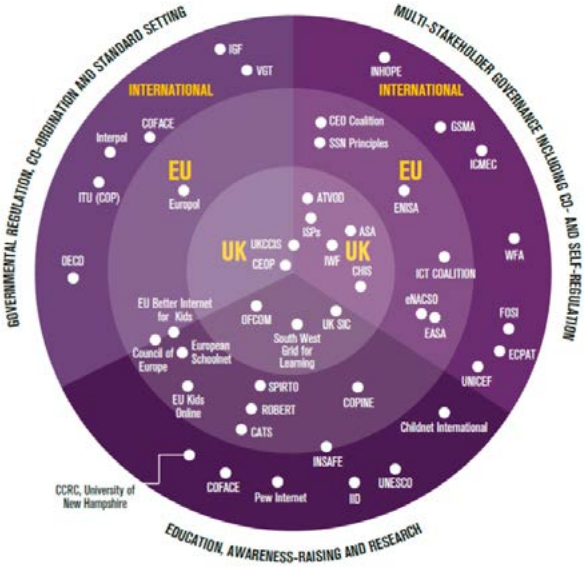
- Is there a comprehensive strategic and co-ordinated multi-stakeholder approach in place?
- Are all relevant stakeholders informed and engaged? These stakeholders include:
  - national, regional and local law-enforcement and other authorities
  - educational and social service agencies
  - independent human rights institutions
  - data protection authorities
  - media and communication regulators
  - professionals working for and with children
  - civil society, including relevant NGOs and child and youth-led organisations

23. See also: Parenting in the Digital Age, published by the Council of Europe in 2020.

  - business enterprises
  - industry associations
  - research institutions
  - political parties
  - trade unions
  - professional associations
  - families
  - children
- Is there an authority designated or a co-ordinating mechanism to assess developments in the digital environment that might impact the rights of the child and which includes children in its decision-making processes, and to ensure that their national policies adequately address such developments?
- Have co-operation frameworks, procedures and processes been set up between competent State authorities, independent authorities, civil society and business enterprises, taking into account their respective roles and responsibilities, capacities and resources?
- Are platforms or providers of communication services required to take prompt and effective action in response to complaints of online violence or abuse by adults or children (including peer-to-peer) or other rights violations, and to co-operate with national authorities?
- Are business enterprises, such as internet service providers and social network providers, engaged to play an active role in preventing and deleting illegal content, as determined by law or by a judicial or other competent authority or reported by the child himself/herself?
- Are civil society stakeholders, as key catalysts in promoting the human rights dimension of the digital environment, encouraged to actively monitor, evaluate and promote children's skills, well-being and related information literacy and training initiatives, including actions undertaken by other stakeholders, and to disseminate their findings and results?
- Are professional media outlets, and public service media in particular, encouraged to be attentive to their role as an important source of information and reference for children, parents or caregivers, and educators in relation to the rights of the child in the digital environment, with due regard to international and European standards on freedom of expression and information and freedom of the media?
- Does the state have a digital inclusion policy that provides access and support to families and children who are excluded from basic digital access, skills and attitudes? Does the state involve libraries, poverty organisations and digital and media literacy organisations for this?

It may be helpful to map the relevant stakeholders to identify different sectors and their interrelations.

Example of a stakeholder map: A guide to stakeholders (EU Kids Online)[24]



4. Fundamental principles

The best interests of the child

According to the UN Committee on the Rights of the Child, the 'best interests principle', laid down article 3 UNCRC, entails that every legislative, administrative and judicial body or institution must systematically consider how children's rights and interests are or will be affected by their decisions and actions.[25]

In its General Comment No. 14, the Committee clarified that the "child's best interests" is a **threefold** concept, i.e.,

- a *substantive right*: the right of the child to have his or her best interests assessed and taken as a primary consideration when different interests are being considered in order to reach a decision on an issue and an intrinsic obligation for States to guarantee that this right will be implemented whenever a decision is to be made concerning a child, a group of identified or unidentified children or children in general,
- a *fundamental interpretative legal principle*: the interpretation which most effectively serves the child's best interests should be chosen if a legal provision is open to interpretation, and

24. See Media@LSE.
25. UN Committee on the Rights of the Child (2003) General Comment No. 5 general measures of implementation of the Convention on the Rights of the Child. CRC/GC/2003/5.

- a *rule of procedure*: whenever a decision is to be made that will affect a specific child, an identified group of children or children in general, the decision-making process must include an evaluation of the possible impact (positive or negative) of the decision on the child or children concerned.[26]

Hence, every decision and action that may have repercussions on a wide array of children's rights in the digital environment should actively take into account the child's best interests. As the digital environment is such an inherent part of children's lives, with the potential to – both positively and negatively – impact their rights, a balanced assessment of children's interests should be at the centre of policymaking and decision-making practices.

Non-exhaustive and non-hierarchical list of elements to be taken into account when assessing and determining the child's best interests[27]

- The child's views
- The child's identity: children are not a homogeneous group and therefore diversity must be taken into account when assessing their best interests
- Preservation of the family environment and maintaining relations
- Care, protection and safety of the child
- Situation of vulnerability
- The child's right to health
- The child's right to education

The UN Committee on the Rights of the Child also asserts that States are required to ensure that the best interests of the child have been assessed and taken as a primary consideration in decisions and actions taken by the private sector (see Chapter 5).[28]

Relevant documents

United Nations Convention on the Rights of the Child, article 3

UN Committee on the Rights of the Child (2013) General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14

Council of Europe, The best interests of the child – A dialogue between theory and practice

26. UN Committee on the Rights of the Child (2013) General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14.
27. UN Committee on the Rights of the Child (2013) General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14: "It should be emphasized that the basic best-interests assessment is a general assessment of all relevant elements of the child's best interests, the weight of each element depending on the others. Not all the elements will be relevant to every case, and different elements can be used in different ways in different cases."
28. UN Committee on the Rights of the Child (2013) General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14, para. 14).

The evolving capacities of the child

The implementation of the rights of the child, also in the digital environment, should take account of children's development and their evolving capacities. For instance, the UN Committee on the Right of the Child has stated that "approaches adopted to ensure the realization of the rights of adolescents differ significantly from those adopted for younger children".[29] The Committee defines evolving capacities as "an enabling principle that addresses the process of maturation and learning through which children progressively acquire competencies, understanding and increasing levels of agency to take responsibility and exercise their rights".[30]

From the perspectives of law and policy, children are (for the most part) defined in terms of chronological age – and the age threshold selected varies depending on the purpose of the law or policy in question (for example, consent to sexual activity, consumption of alcohol and tobacco, army enlistment or leaving school). Often, those tasked with the responsibility of creating such laws and policies do not elaborate on the actual reasoning behind the selection of particular age thresholds for particular purposes and – in the absence of such hypotheses – choices can appear arbitrary. Laws and policies restricting children's access to certain types of media content (on the basis that it is harmful to children who have not attained a certain age) impact on children's exercise of their right to freedom of expression and receive information and, for this reason, the imposition of age limits should be justified and evidence-based. Children's understanding of the nature and operation of the digital environment depends not only on their evolving capacities but also on the transparency and design of that environment.[31]

The right to non-discrimination

UNCRC article 2.1 asserts that the rights of the child apply to all children without discrimination on any grounds. It specifies in particular that there should be no discrimination – intentional or inadvertent – on the basis of "the child's or his or her parents' or legal guardians' race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth, or other status." In preparing the Recommendation it was recognised that this is a non-exhaustive list and that in specific contexts, other forms of discrimination might occur.

The non-discrimination principle forbids situations "where persons or groups of people in an identical situation are treated differently, and where persons or groups of people in different situations are treated identically".[32] This includes 'direct discrimination', entailing that individuals who are in similar situations are treated less

29. UN Committee on the Rights of the Child (2016) General Comment No. 20 on the implementation of the rights of the child during adolescence, CRC/C/GC/20, para 1.
30. UN Committee on the Rights of the Child (2016) General Comment No. 20 on the implementation of the rights of the child during adolescence, CRC/C/GC/20, para 18.
31. For an account of child development in relation to the digital environment, see Kidron and Rudkin Digital Childhood (2018); for an account of how children's understanding depends on service transparency and design, see Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age.
32. European Union Agency for Fundamental Rights and Council of Europe (2018) Handbook on European non-discrimination law.

favourably simply because of a particular 'protected' characteristic that they possess, as well as 'indirect discrimination', where treatment based on a seemingly neutral rule disadvantages a person or a group of persons as a result of their particular characteristic.[33] Note that the Recommendation also states there should be no discrimination on the basis of the child's age.

To fulfil the child's right to non-discrimination, it is important that member States should:

- make every effort to respect, protect and fulfil the rights of each and every child in the digital environment
- identify specific forms of discrimination relevant to their own country or culture
- apply targeted measures as needed for children in vulnerable situations, recognising that the digital environment has the potential both to increase children's vulnerability and to empower, protect and support them.[34] The UN Committee on the Right of the Child has stated that the "*non-discrimination obligation requires States actively to identify individual children and groups of children the recognition and realization of whose rights may demand special measures*".[35]

Relevant documents

United Nations Convention on the Rights of the Child, article 2

Council of Europe Convention on Human Rights, article 14

The right to be heard

The right to be heard, included in article 12 UNCRC, is another one of the four general principles of the UNCRC and ascribes to children the right to be heard and have their views taken seriously in all matters affecting them, to participate in all decision-making processes having a bearing on their lives, and to exert influence over such decisions in accordance with their age and maturity. It places an obligation on States to truly involve children in all matters affecting them.

According to the Committee on the Rights of the Child:

> *"The views expressed by children may add relevant perspectives and experience and should be considered in decision-making, policymaking and preparation of laws and/or measures as well as their evaluation […] The concept of participation emphasizes that including children should not only be a momentary act, but the starting point for an intense exchange between children and adults on the development of policies, programmes and measures in all relevant contexts of children's lives."*[36]

33. European Union Agency for Fundamental Rights and Council of Europe (2018) Handbook on European non-discrimination law.
34. In this respect, a report by the Council of Europe on "Children with disabilities in the digital environment" was published in 2019.
35. UN Committee on the Rights of the Child (2003) General Comment No. 5 general measures of implementation of the Convention on the Rights of the Child. CRC/GC/2003/5.
36. United Nations Committee on the Rights of the Child, General Comment No. 12 (2009) on the right of the child to be heard.

Inspired by the UNCRC and its own standards and previous practice, children have also been consulted in the preparation of the Recommendation underlying this Handbook. Member States' governments and all other stakeholders should allow for the participation of children in policymaking processes surrounding the digital environment. A child-friendly version of the Recommendation was published and be made widely available (including via the internet) in June 2020.

Child participation: useful references from the Council of Europe

Council of Europe Recommendation on participation of children and young people under the age of 18

Council of Europe Child Participation Assessment Tool (CPAT) & Implementation Guide (2016)

See further the Council of Europe webpage on children participation

Concrete participation mechanisms that can be used include, for example:

- youth councils, forums or parliaments
- online platforms where children can share views, vote on statements, comments on proposals
- co-creation or co-design workshops facilitated by professional moderators

The Council of Europe Advisory Council on Youth

The Advisory Council on Youth is the non-governmental partner in the co-management structure which establishes the standards and work priorities of the Council of Europe's youth sector and makes recommendations for future priorities, programmes and budgets. It is made up of 30 representatives from youth NGOs and networks in Europe and its main task is to advise the Committee of Ministers on all questions relating to youth.

Participation must be:

- transparent and informative
- voluntary
- respectful
- relevant
- child-friendly
- inclusive
- ethical
- supported by training for adults
- safe, without putting children at risk
- accountable[37]

37. Council of Europe Child Participation Assessment Tool (CPAT), Appendix, p. 28. Note that child participation activities should take place under a child safeguarding policy set up by lead organisations.

Important! Engaging with children and child safeguarding

Organisations which engage with children must ensure that they are safeguarded against any form of abuse. According to UNICEF, child safeguarding "*refers to all of the actions [an organisation] takes to keep all children they come into contact with safe – and includes proactive measures put in place to ensure children to not come to harm as a result of any direct or indirect contact with the company. Child safeguarding encompasses the prevention of physical, sexual and emotional abuse, neglect and maltreatment of children by employees and other persons whom the [organisation] is responsible for, including contractors, business partners, visitors to premises and volunteers*".[38]

Organisations which come into contact with children, including to hear their views, should have a child safeguarding policy in place.

Relevant documents

United Nations Convention on the Rights of the Child, article 12

United Nations Committee on the Rights of the Child, General Comment No. 12 (2009) on the right of the child to be heard

UNICEF (2018) Child safeguarding toolkit for business

38. UNICEF (2018) Child safeguarding toolkit for business.

Chapter 3

Operational principles in practice

This chapter suggests how six areas of operational principles and measures that are included in the appendix of the Recommendation can be put into practice.

Human rights are indivisible and interconnected. For these reasons, they should not be ranked in terms of priorities; rather, the Recommendation calls for the importance of a holistic and coordinated approach to realising the full array of the rights of the child in the digital environment. For example, if measures are taken to protect children from the risk of harm without, at the same time, considering their right to freedom of expression, protective measures may be adopted that are overly restrictive of expression rights.

Note that since the internet is subject to continuous and fast change, there have been few independent evaluations of what works or does not work. For this reason, the handbook invites States to work towards their own good practice; it will include examples of good practice in a future publication.[39]

Questions / checklist for member States

For every measure taken under each operational principle, you should check the following questions addressing cross-cutting issues to be considered in any policy-making in favour of children:

- have children been consulted?
- have you reviewed the evidence?
- have you engaged the relevant stakeholders?
- have you considered vulnerable groups?
- have you provided specific remedies for children?
- have you identified the relevant law / framework / action plan?

1. Access to the digital environment

Access to and use of the digital environment is important for the realisation of children's rights and fundamental freedoms, for their inclusion, education, development, participation and for maintaining family and social relationships. Where children do not have access to the digital environment or where this access is limited as a result of poor connectivity, their ability to fully exercise their human rights may be affected.

39. It may be helpful to consider UNICEF's Implementation Handbook for the Convention on the Rights of the Child.

Increasingly, in consultations with children themselves, they view access to the digital environment as vital for their well-being. Although in general human rights documents, access to the internet is not yet recognised as a specific right, there have been discussions at the level of the United Nations, which have acknowledged that States do have 'a positive obligation to promote or facilitate the right to freedom of expression and the means necessary to exercise this right, which includes the internet'.[40] This approach is strengthened by state decisions to provide vital public services primarily online, and by evidence of social inequalities which are exacerbated by digital exclusion.

Policy and provision for access often falls under the remit of the ministry for industry or business or infrastructure. It will be important that States ensure that the relevant ministry is sufficiently informed about children's needs and rights, including the potential for provision, through unintended consequences, to exacerbate risks and inequalities for children. Access to technology is of little value without the necessary digital skills and literacies to make use of the technology wisely, safely, and meaningfully.[41] This means that access should be addressed together with education and training, as discussed in section 3.5.

In the history of technological innovation, the wealthiest in any society generally gain access first to the latest technologies, as well as the knowledge to use them. For children especially, one source of exclusion or disadvantage tends to compound another, making it particularly important that the most marginalised children are specifically included in policies to improve access. Insofar as access to the digital environment mediates children's access to information and education, among other rights, the importance of non-discrimination should be at the forefront of state decision-making and provision regarding access. For many children, access may be personal, or provided at home or school. For children lacking ready access at home or school, cybercafés may be important though these are not always safe for children; libraries, youth clubs and other public places can play a key role in providing access.

Access to the digital environment in school settings can be provided in a variety of different ways, for instance by providing computers and tablets in classes or by adopting bring-your-own-device policies (for instance tablets, smart phones, gaming devices or virtual reality headsets). Policies about how such devices can be used in particular settings are useful and should be developed with participation by children.

Moreover, and increasingly, access to services in the digital environment is offered on the condition that personal data is handed over. In such situations, data protection principles, as described in 3.4., should be respected. States should be mindful of evolutions that move towards a new divide in society where those who can afford to pay will not need to provide personal data and those who cannot will. It has been acknowledged, for instance by the European Data Protection Supervisor, that "fundamental rights such as the right to the protection of personal data cannot be not be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity".[42]

---

40. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue), 'Report on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the internet' (2011) UN Doc A/66/290.
41. On meaningful access, see UNICEF (2017) Access to the Internet and Digital Literacy.
42. European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content.

Questions / checklist for member States

- Are there appropriate arrangements in place to ensure that all children have adequate, affordable and secure access to devices, connectivity, services and content which is specifically intended for children?
- Is access to the digital environment provided safely and free of charge in dedicated public spaces which children can use?
- Is access to the digital environment provided in educational and other care settings for children?
- Are specific measures taken for children in vulnerable situations, in particular children with disabilities, children living in alternative care, children deprived of liberty or whose parents are deprived of liberty, children in the context of international migration, children in street situations, children in rural communities and children otherwise living with limited economic resources?
- Are online service providers required to ensure that their services are accessible by children with disabilities (mental or physical disabilities)?
- Is connectivity and access to devices, services and content accompanied by appropriate education and literacy measures, including those which address gender stereotypes or social norms that could limit children's access and use of technology?
- Are there measures in place that ensure that terms and conditions that are associated with the use of a device which can connect to the internet or that apply to the provision of online services or content are accessible, fair, transparent, intelligible, available in the child's language and formulated in clear, child-friendly and age-appropriate language where relevant?
- Are there measures in place that ensure a plurality of sources of high-quality information and educational digital content and services for children?
- Are children's rights taken into account in public procurement procedures, for instance for educational tools, so that access to and use of digital services and content is not unduly restricted by commercial interests or filters?

Controversy over "screen time"

There is controversy in public and expert domains over whether "too much" access to digital technologies, especially screen-based media, is problematic for children. In many countries, there is active consideration of whether children's access should be limited – by age (especially for pre-school children), by time of day (especially at night) or in certain places (especially at school). States will need to keep under review the latest evidence regarding the impact of using digital technologies on children's physical and mental health. The difficulty lies in weighing the sheer quantity versus the quality of children's screen time, with the quality depending on the activities they engage in, with whom, under what conditions and with what beneficial or harmful effects.

Relevant binding and non-binding instruments
Recommendation, section 3.1.

United Nations, Convention on the Rights of the Child (UNCRC), article 17

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users

2. Right to freedom of expression and information

The digital environment has considerable potential to support the realisation of children's right to freedom of expression, including to seek, receive and impart information and ideas of all kinds. Children can express themselves and receive information through social media accounts, groups and pages, blogs, (news) websites, digital communication channels of youth or interest groups, video-sharing platforms, online counselling or helplines, online health-related information resources and so forth.

The Council of Europe's (2016) Strategy on Internet Governance notes that:

> *"Individuals rely on the Internet for their everyday activities and more and more people have access to online services. For many, including children and young people, it is their primary source of information and means of expression. The Internet is therefore an invaluable space for the exercise of fundamental rights such as freedom of expression and information."*

The right to freedom of expression is not an absolute right. It carries with it duties and responsibilities. It can also be restricted, but any restriction must (1) be prescribed by law, (2) have a legitimate aim, and (3) be necessary in a democratic society.[43] This means that children's right to freedom of expression and information can be limited, in order to protect their interests (e.g. restricting access to content that is considered harmful to them by means of internet filters or systems of age verification), or in order to protect the interest of others (e.g. restricting online hate speech towards others). These restrictions must fulfil the three conditions mentioned above.

Measures that are proposed and taken to try to ensure that children do not come across content that is considered harmful to them may be legitimate but should be carefully considered. The proportionality of the measure should be assessed, taking into account the age and maturity of the child, as well as its effectiveness.

Important!

- Children must be made aware of restrictions.
- Children must be made aware of the consequences of their behaviour on the Internet vis-à-vis their peers.
- Children must have a remedy to address restrictions that are deemed illegitimate by them (e.g. submit a complaint regarding the unjustified removal of a picture).

As regards the right to information, the UN Committee on the Rights of the Child (CRC/C/GC/12 2009) stated that:

> *"Children need access to information in formats appropriate to their age and capacities on all issues of concern to them. This applies to information, for example, relating to their rights, any proceedings affecting them, national legislation, regulations and policies, local services, and appeals and complaints procedures".*

43. Article 10 ECHR.

In large part, businesses may already provide a plurality of information sources of value to children, and this is to be encouraged, for instance through the provision of incentives. However, in small language communities, or for certain population segments, provision may be sparse. It may also be judged, in certain circumstances, that the available information lacks sufficient diversity, is overly commercialised or not provided in a child-friendly manner. Moreover, high-quality content might not always be easy to find for children. Search functionalities and algorithms may be biased or personalised, to the extent that finding less popular or poorly indexed but valuable information might be hampered.

Thus, public service media or other public or civil society bodies may be required to supplement already-available sources so as to provide for children's information rights. Such actions might take the form of public funding or incentives for the provision of particular kinds of content. It might also involve support for child-friendly search facilities or portals so that high quality content can be readily found by children. Children's information access should not, however, be restricted to using particular portals or services.

Children's right to sex and relationships information

In some cultural contexts, children's access to information about sexual health, sexual experiences or sexual identity is controversial. In the digital environment, it can be difficult to draw a clear line between sexual contents that are harmful to children and those which provide information, or which allow for expression. It is important to take into account children's own views and evolving capacities when determining provision, as well as evidence regarding the possible costs to their well-being of restricting access to needed sexual information, especially during adolescence. The rights of young people as they approach the age of sexual consent require special consideration. Relevant programmes for sex and relationships education, including with regard to the digital environment, should be established as part of compulsory official school curricula.[44]

Questions / checklist for member States

- Is there a framework in place that guarantees the child's right to hold and express any views, opinions or expressions on matters of importance to them, through the media of their choice, and irrespective of whether or not their views and opinions are received favourably by the State or other stakeholders?
- Are restrictions on the child's freedom of expression in the digital environment prescribed by law, do they intend to achieve a legitimate aim and are they necessary in a democratic society?
- Are children informed of restrictions that are in place in a manner appropriate to their evolving capacities? (E.g. internet filters or systems of age verification)

44. Resources were developed under the former Council of Europe Pestalozzi Programme.

- Are children provided with guidance on appropriate remedies with regard to restrictions on their right to freedom of expression, including on how and to whom to make a complaint, report an abuse or request help and counselling? Are parents informed thereof?
- Are children provided with guidance on how they can exercise their right to freedom of expression while respecting the rights and dignity of others? Are they informed that their right to freedom of expression might be restricted because of intellectual property rights of others or because their expression incites to hatred or violence?
- Does the state initiate and encourage the provision of diverse high-quality online content and services of social and cultural benefit to children in support of their fullest development and participation in society? Is there high-quality content that is specifically made for children, easy for them to find and understand, provided in their language, and adapted to their age and maturity?
- Can children easily find high-quality information on the rights of the child, including in the digital environment, on news, on health, and on sex and relationships?
- Is there high-quality public service media content available for children?
- Where provision is made for media, are children involved in active forms of communication, encouraging the provision of user-generated content and establishing other participatory schemes?
- Is attention paid to children's access to, and presence and portrayal in, media online?

Relevant legislative instruments

United Nations, Convention on the Rights of the Child (UNCRC), article 13 and 17

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, article 10

Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership

Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users

Recommendation CM/Rec(2012)1 of the Committee of Ministers to member States on public service media governance

Relevant case law of the European Court of Human Rights

Fact sheet: Access to Internet

Fact sheet: Hate speech

Fact sheet: Protection of reputation

3. Participation, right to engage in play and right to assembly and association

The digital environment provides distinctive opportunities for the rights of the child to participate, to engage in play and to peaceful assembly and association, including through online communication, gaming, networking and entertainment. Especially in the digital context, play and association are crucial to a child's identity and healthy development, and so opportunities must be provided in children's own language, in ways that validate and recognise their culture and heritage and which support belonging. Hence, play and association in the digital environment should be made accessible to all children. At the same time, a healthy balance should be promoted between children's online and offline activities as also shown through the Council of Europe's new Digital Parenting Guide.[45]

The concept of child participation is complex and multifaceted: it encompasses the right to be heard in schools and other places, within judicial proceedings, or in political decisions which affect them, as well as the right to socio-economic participation and inclusion and access to equal opportunities. All of this allows children to develop and become engaged in democratic citizenship, at a pace which matches their level of maturity and understanding. Digital technologies do not only enhance children's chances to make their voices heard in certain contexts, they also provide children with new opportunities for taking part in social and other activities.

Two key provisions of the UN Convention on the Rights of the Child (UNCRC) underly this concept:

Article 12 UNCRC requires 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."

Article 15 UNCRC requires that "States Parties recognize the rights of the child to freedom of association and to freedom of peaceful assembly."

The Council of Europe Guide to Human Rights for Internet Users explains how these rights apply – in fact to all users – in digital environments:

1. *"You have the freedom to choose any website, application or other service in order to form, join, mobilise and participate in social groups and assemblies whether or not they are formally recognised by public authorities. You should also be able to use the Internet to exercise your right to form and join trade unions;*
2. *"You have the right to protest peacefully online. However, you should be aware that, if your online protest leads to blockages, the disruption of services and/or damage to the property of others, you may face legal consequences;*
3. *"You have the freedom to use available online tools to participate in local, national and global public policy debates, legislative initiatives and public scrutiny of decision-making processes, including the right to sign petitions and to participate in policy-making relating to how the Internet is governed."*

45. Parenting in the Digital Age - Positive parenting strategies for different scenarios, August 2020.

Questions / Checklist for member States

- Do you co-operate with other stakeholders to provide for access of children to such activities that can foster participation, inclusion, digital citizenship and resilience both online and offline, thereby promoting children's civil and democratic participation according to their evolving capacities?
- Is a range of incentives, investment opportunities, standards and technical guidance provided for the production and distribution of digital content and services of social, civic, artistic, cultural, educational and recreational benefit to all children? This includes, for example, interactive educational and play-based tools that stimulate skills such as creativity, teamwork and problem solving appropriate to their evolving capacities and with particular attention to the needs of children in vulnerable situations.
- Is particular attention paid to the participation of vulnerable groups of children (including, for example, children with disabilities)?
- Is information appropriate to their age and maturity provided to children, including in non-written forms and through social networking and other media, on their rights, in particular their participation rights?
- Are children adequately informed of the opportunities available to them, and where they can get support to take advantage of these opportunities?
- Where children participate in the creation or production of digital content, services or tools, are there measures in place to protect the child's intellectual property rights?
- Are measures taken to ensure that children are able to participate effectively in local, regional national and European or international public-policy and political debates and to support the development of online civic and social platforms to facilitate their participation and their enjoyment of the right to assembly and association, strengthening their capacity for democratic citizenship and political awareness?
- Is children's participation in the digital environment addressed and acted upon meaningfully, building on existing good practice for child participation and available tools for assessment?
- Are measures taken to protect children exercising their right to peaceful assembly and association in the digital environment from monitoring and surveillance, whether carried out by State authorities directly or in collaboration with private sector entities?
- Where such measures interfere with the exercise by children of their rights, are they subject to conditions and safeguards against abuse, in line with international and European human rights conventions and standards? Are they prescribed by a law which is accessible, precise, clear and foreseeable, pursue a legitimate aim, are they necessary in a democratic society and proportionate to the legitimate aim pursued, and do they allow for effective remedies?
- Do actions in support of children's rights to participation, play, assembly and association include appropriate child safeguarding policies and methodologies for evaluation as well as feedback from/to participating children?

Relevant binding and non-binding instruments

Recommendation 3.3

United Nations, Convention on the Rights of the Child (UNCRC), article 12 (right to be heard, article 15 (assembly) & article 31 (play))

United Nations, General Comment No. 17 (2013) on the right of the child to rest, leisure, play, recreational activities, cultural life and the arts (article 31)

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, article 11 (assembly and association)

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users

4. Privacy and data protection

Children have a right to private and family life in the digital environment, which includes the protection of their personal data and respect for the confidentiality of their correspondence and private communications. The EU's Fundamental Rights Agency's 'Handbook on European law relating to the rights of the child' (2015) observes that:

> *"Under international law, the right to data protection is part of the child's right to privacy contained in Article 16 of the CRC. This article provides that a child shall not be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. This right must be* **respected by everybody, including the child's legal representative.***" (p. 193; emphasis added)*

It is the primary obligation of the State to respect, protect and fulfil the right of the child to privacy and data protection. This entails that a legal framework must be in place. Such a framework may include:

- a constitutional provision guaranteeing the right to data protection and to privacy which also applies to children (reference to article 16 UNCRC, article 8 ECHR, article 7 CFREU and article 8 CFREU), and ensuring that restrictions of these rights must be in accordance with the law, pursue a legitimate aim, and be necessary in a democratic society,
- a national data protection law/framework.

What are personal data?

Personal data = any information relating to an identified or identifiable individual ("data subject")

Examples of personal data:

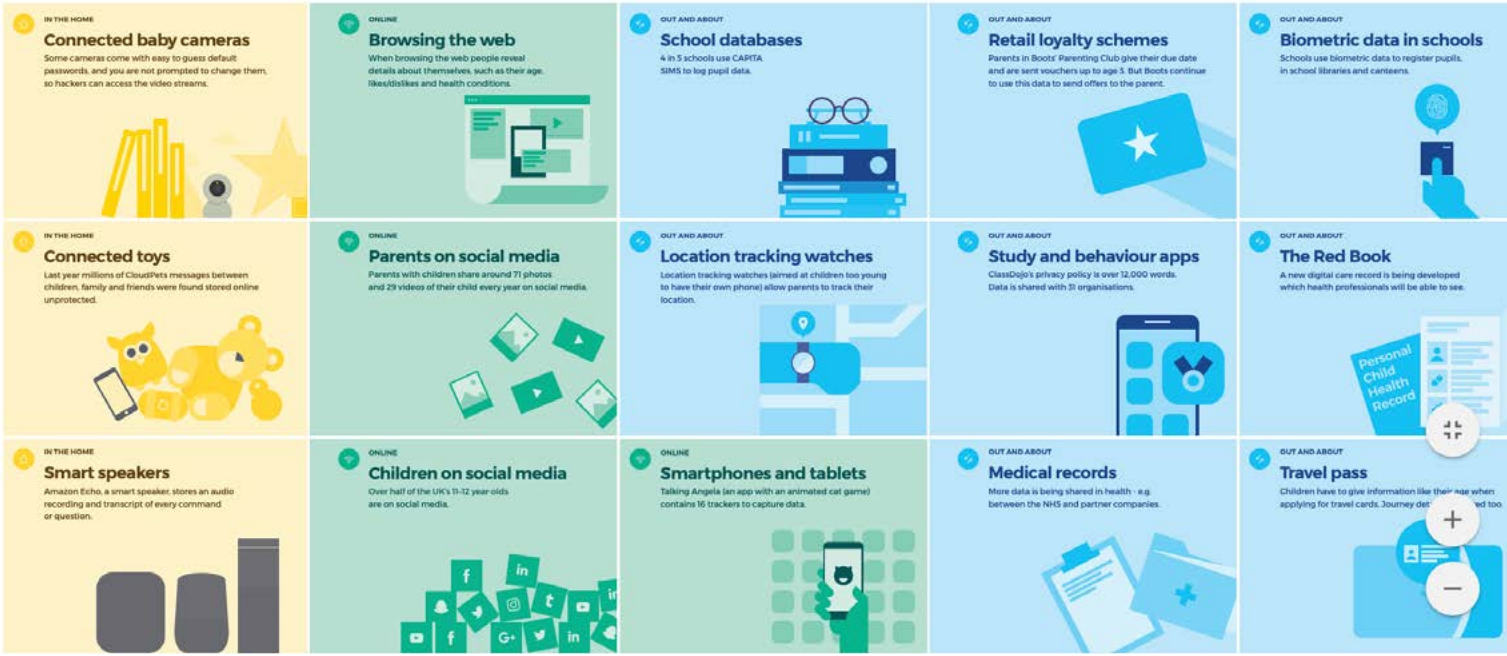
- a name and surname;
- a home address or telephone number;
- an email address;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- a cookie ID.

Certain categories of data are considered **special categories of data**, subject to stricter requirements:

genetic data, biometric data uniquely identifying a child, personal data relating to criminal convictions, and personal data that reveal relating racial or ethnic origins, political opinions, religious or other beliefs, mental and physical health, or sexual life.

Collection of personal data of children

Children are increasingly the subject of data collection practices. The following infographic visualises the various domains in which this occurs, and which actors are involved.



Source: Children's Commissioner, Who knows what about me? *Infographic*, 2018.

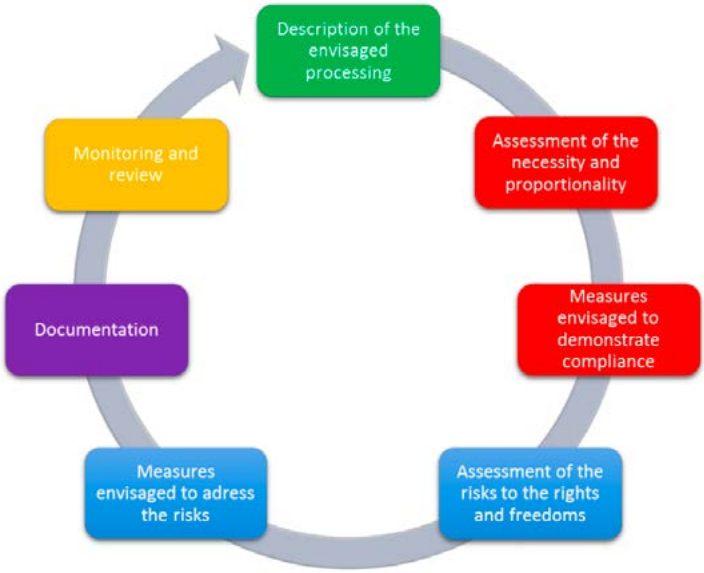
Checklists for member States

A (national) data protection law should include:

- measures to ensure that children's personal data is processed fairly, lawfully, accurately and securely, for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents, caregiver or legal representative, or in accordance with another legitimate basis laid down by law;
- the data minimisation principle, meaning that personal data processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed;
- data protection impact assessment mechanisms that ensure that the likely impact of intended data processing on the rights of the child is assessed and that the data processing is designed to prevent or minimise the risk of interference with those rights.

A Data Protection Impact Assessment

This is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).



Source: Article 29 WP (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

A (national) data protection law should also include:

- restrictions on the processing of special categories of data that are considered sensitive (i.e. genetic data, biometric data uniquely identifying a child, personal data relating to criminal convictions, and personal data that reveal racial or ethnic origins, political opinions, religious or other beliefs, mental and physical health, or sexual life)
- rights for data subjects, such as the right to withdraw their consent to the processing of their personal data, have access to their personal data and to have it rectified or erased, notably when the processing is unlawful or when it compromises their dignity, safety or privacy
- requirements to provide easily accessible, meaningful, child-friendly and age-appropriate information on how data is collected, stored, used and disclosed, on their rights to access their data, to rectify or erase this data or object to its processing, and how to exercise their rights
- requirements on the implementation of privacy-by-default and privacy-by-design measures, taking into account the best interests of the child
- a prohibition of profiling of children (i.e. any form of automated processing of personal data which consists of applying a "profile" to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes), unless this is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by the law
- the establishment of an independent data protection authority

Profiling

Profiling is an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. Profiling can be carried out for a variety of reasons, such as health reasons or marketing or advertising purposes.

Profiling is sometimes used to make **automated decisions** about an individual. According to Convention 108+, however, every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.

The Committee of Ministers has acknowledged in its Recommendation that profiling of children may have serious consequences for them throughout their life, and given that they are unable, on their own behalf, to give their free, specific and informed consent when personal data are collected for profiling purposes, **specific and appropriate measures for the protection of children** are necessary to take account of the best interests of the child and the development of their personality in accordance with the UNCRC.[46]

46. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

When establishing or reviewing a national data protection framework, States should pay particular attention to:

- ensuring child participation in the design or review process
- determining the age at which a child can consent to the processing of his or her personal data: in deciding on this age, children's rights, views, best interests and evolving capacities must be taken into consideration ; this should be monitored and evaluated while taking into account children's actual understanding of data collection practices and technological developments
- ensuring that adequate information is provided to children on their rights, responsibilities, risks and remedies in case of violations of their rights
- ensuring that where children are considered too young to consent, and thus parental consent is required, reasonable efforts are made to verify that consent is given by the parent or legal representative of the child
- avoiding prohibiting in law or practice anonymity, pseudonymity or the usage of encryption technologies for children
- determining and ensuring whether and how the framework that is in place is applicable to new or emerging technical phenomena, such as smart and connected toys and devices that are aimed at children or that are used in proximity of children, or increasing use of algorithms and deployment of artificial intelligence

In the Explanatory Memorandum to the Guide to human rights for Internet users, it has been acknowledged that "*in order to ensure protection against online surveillance and to enhance freedom of expression, Council of Europe member States should respect the will of Internet users* ***not to disclose their identity****. However, respect for anonymity does not prevent member States from taking measures in order to trace those responsible for criminal acts, in accordance with national law, the ECHR and other international agreements in the fields of justice and the police*".[47]

For children in particular, anonymity might be crucial in their development and the shaping of their identity, for instance when they are searching for information about sexuality. This might mean anonymity from the State, from service providers or from parents. Moreover, children should also be able to report content and behaviour which poses a risk of harm, and to receive advice and support, with due regard to their confidentiality and anonymity.[48] Pseudonymity, on the other hand, might also be a useful strategy for children to navigate the digital environment, for instance by using usernames that are not linked to their real names.

47. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, point 59.
48. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, point 95.

Smart and connected toys and devices

An emerging concern relates to the way in which the Internet of Things (IoT) and, in particular, the Internet of Toys, affects children. New smart and connected toys directed at children (such as dolls, robots and watches) provide many positive opportunities for children, such as entertainment, enjoyment and reassurance, (informal) learning, identity-building and self-development. Yet, such devices may also pose serious risks to children's rights to privacy and data protection. These include corporate and government surveillance, data privacy and security issues, geolocation tracking, remote control of technologies and security failures. Moreover, connected toys are not the only internet connected devices that children are using today. Other IoT devices that impact children's lives and rights, such as smart home assistants, which are not directly targeted at children, but are present in their home environments, should also be the subject of regulatory compliance checks.

Other action points for member States include awareness-raising:

- Towards *children*: ensuring that children know how they can exercise their right to privacy and data protection, taking into account their age and maturity, and, where appropriate, with the direction and guidance of their parents, caregivers, legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child
- Towards *parents*: ensure parents have up to date information (for instance, advice related to keeping the computer in the living room is less relevant today, as children use devices that are easily portable such as tablets and smart phones), a helpline or similar, access to advice and training to develop their own skills

Sharenting

Parents are not only crucial in protecting their child's privacy online, but they may also pose a risk to their privacy. Sharenting is a word that is made up of 'sharing' and 'parenting'. It refers to the phenomenon of parents sharing information about their children, photographs for example, on blogs or social media, such as Facebook, Instagram or YouTube. Of course, most parents do this with good intentions, because they are proud of their children, or because they want to share experiences with other parents about the wonderful but sometimes also difficult aspects of being a parent. Some parents share only occasionally, other parents share almost everything that happens in their daily lives. Children, especially as they grow older, do not always feel comfortable with the information that their parents share. Sometimes conflicts arise between the child's right to privacy and the right to freedom of expression of the parent. Whatever the circumstances, parents should keep the best interests of the child in mind and discuss with their child what they share and why.

- Towards *business enterprises*:[49] member States should foster a business culture that respects and supports children's rights to privacy and data protection, encouraging business enterprises to integrate their responsibility into their

49. See also Chapter 5: Engaging with business enterprises.

internal by-laws and procedures, core values, policies and strategies. This can be done by proactively engaging with companies directly or through other channels, such as chambers of commerce, industry groups, professional societies and other business associations (UNICEF & ICJ, 2015)

Relevant binding and non-binding instruments

Recommendation, section 3.4

United Nations, Convention on the Rights of the Child (UNCRC), article 16

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, article 8

Council of Europe, Modernised Convention 108 for the Protection of Individuals with regard to the Processing of Personal Data

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users

Recommendation CM/Rec(2010)13 on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling

Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Guidelines on Artificial Intelligence and Data Protection

European Union, General Data Protection Regulation

General Data Protection Regulation

The General Data Protection Regulation was adopted in 2016 by the European Union and applies since 25 May 2018. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. The Regulation build on principles, obligation and rights that are included in Convention 108 (+)

See also information on Data Protection in the EU and on the EU Data Protection Rules

Relevant case law of the European Court of Human Rights

Fact sheet, Personal data protection

Fact sheet, Right to the protection of one's image

Relevant additional resources

FRA (2018) Handbook on European data protection law

HELP Course Data Protection and Privacy Rights

5. Right to education

States should actively invest in and promote the opportunities offered by the digital environment to realise children's right to education. The goal of education is the development of the child's personality, talents and mental and physical abilities to their fullest potential, and the preparation of the child for a responsible life in a free society. In support of this goal, it is important that the knowledge and resources of the digital environment are available to all children in a way that is inclusive and takes into account children's evolving capacities and the particular circumstances of children in vulnerable situations (Guidelines, point 40). Provision for children's education in and about the digital environment can be ensured through the actions of a wide range of formal, nonformal and informal learning organisations. This should include educating children about their rights in the digital environment.

> *"You have the right to education, including access to knowledge. This means:*
>
> *1. "You should have online access to education and to cultural, scientific, scholarly and other content in official languages. Conditions might apply to such access in order to remunerate rights' holders for their work. You should also be able to freely access publicly funded research and cultural works in the public domain on the Internet, where available;*
>
> *2. "As part of Internet and media literacy you should have access to digital education and knowledge in order to exercise your rights and freedoms on the Internet. This includes skills to understand, use, and work with a broad range of Internet tools. This should enable you to critically analyse the accuracy and trustworthiness of content, applications and services that you access or wish to access."*
>
> *(Council of Europe Guide to Human Rights for Internet Users)*

Questions / Checklists for member States

Digital literacy

- Is there a policy in place that promotes the development of digital literacy, including media and information literacies and digital citizenship education, to ensure that children have the competence to engage in the digital environment wisely and the resilience to cope with its associated risks?
- Is digital literacy education included in the basic education curriculum for all, from the earliest years, and taking into account children's evolving capacities?
- Does digital literacy education include:
  - the technical or functional competences to use a wide range of online tools and resources;
  - skills related to content creation and expression, and
  - the critical understanding of the digital environment, its opportunities and risks?
  - the capacity to reflect on the child's own behaviour, that of others and the use of digital media in society as a whole, to choose the most constructive approach to using digital media for interaction, information, creation, participation and leisure?

- Is digital literacy promoted in the settings where children use the internet, especially schools and organisations working with and for children?
- Is digital literacy of parents or caregivers promoted and supported through the State's established mechanisms for reaching parents?
- Do educational policies that use digital networks to connect formal and non-formal learning, including at home, not disadvantage children who lack resources at home or live in residential institutions?
- Are particular efforts made by States and other relevant stakeholders, through the education and cultural system, to support and promote the digital literacy of children who:
  - have little or no access to digital technology for socio-geographical or socio-economic reasons, as well as sometimes for reasons of place of residence;
  - have access to but do not use digital technology;
  - lack the skills to use or underuse digital technology for reasons of vulnerability, in particular for children with disabilities?
- Are States making efforts to enhance the use of information and communication technology by girls and to promote the equality of opportunities and outcomes for all children?

See: The European Commission's Digital Competence Framework 2.0[50]

DigComp 2.0 identifies the key components of digital competence in 5 areas which can be summarised as below:

1) **Information and data literacy**: To articulate information needs, to locate and retrieve digital data, information and content. To judge the relevance of the source and its content. To store, manage, and organise digital data, information and content.

2) **Communication and collaboration**: To interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity. To participate in society through public and private digital services and participatory citizenship. To manage one's digital identity and reputation.

3) **Digital content creation**: To create and edit digital content To improve and integrate information and content into an existing body of knowledge while understanding how copyright and licences are to be applied. To know how to give understandable instructions for a computer system.

4) **Safety**: To protect devices, content, personal data and privacy in digital environments. To protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion. To be aware of the environmental impact of digital technologies and their use.

5) **Problem solving**: To identify needs and problems, and to resolve conceptual problems and problem situations in digital environments. To use digital tools to innovate processes and products. To keep up-to-date with the digital evolution.

50. See: EC Digital Competence Framework 2.0.

Educational programmes and resources

- Are there measures in place that ensure that sufficient high-quality educational resources, physical devices and infrastructures are available to benefit children's operation in the digital environment and support their formal, non-formal and informal education?
- Have education and awareness-raising initiatives and programmes and user tools been developed and strengthened for children, parents or caregivers, and educators and volunteers working with children, with the involvement of children? Such programmes should include knowledge on:
  - the nature and functioning of the digital environment,
  - preventive measures,
  - rights and responsibilities in the digital environment,
  - identification and reporting of violations,
  - remedies and available redress against any violations encountered,
  - Teaching children to understand, as appropriate according to their age and evolving capacities:
    - what it means to give consent,
    - to respect other fundamental rights, their own and those of others,
    - to seek redress when needed and
    - to use available tools to protect and fulfil their rights in the digital environment
  - Enabling children to be aware of and deal with:
    - potentially harmful content (such as violence and self-harm, adult pornography, child sexual abuse material, discrimination and racism, hate speech) and behaviour (such as the solicitation of children for sexual purposes or "grooming", bullying or harassment, unlawful processing of personal data, violation of intellectual property rights), and
    - potential consequences of the way in which information about children or shared by children might be further disseminated in different settings and by others.
- Are formal and non-formal educational and cultural institutions (including archives, libraries, museums, child and youth-led organisations, and other learning institutions) supported and encouraged to develop and make available a variety of digital and interactive learning resources and to co-operate across institutional boundaries to optimise learning opportunities in relation to the digital environment?

Useful Council of Europe resources:

Council of Europe (2017) Internet Literacy Handbook sets out to provide information and promote reflection on some of the more complex ethical, sociological and cultural issues that are intrinsically linked to digital- and media-related activities which have taken on such a large role in the lives of a majority of people in many parts of the world.

It is presented as a compendium of Fact sheets which are organised into six themed sections, enabling users to more easily download and print section by section or individually, as they wish.

See also:

Digital citizenship education project

Mapping of media literacy practices and actions in EU-28

Relevant binding and non-binding instruments

Recommendation, section 3.5

United Nations, Convention on the Rights of the Child (UNCRC), articles 28 and 29

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users

6. Right to protection and safety

Taking into account the development of new technologies, children have the right to be protected from all forms of violence, exploitation and abuse in or as a result of actions in the digital environment. Mindful of the speed of technological innovation and the speed at which new technology-related practices can emerge, States should assess regularly, based on reliable evidence, the risks of harm that these may pose to children's mental and physical well-being and to the to the respect, protection and fulfilment of their rights. This is especially important because new risks can threaten children's safety before their parents and caregivers, or teachers are aware of them or prepared for them.

Preventative measures are generally preferable to reactive measures, but both are vital. Any precautionary or protective measures should take into consideration the best interests and evolving capacities of the child and not unduly restrict the exercise of other rights, as well as pursue rehabilitative purposes in case of violations committed by children (including peers).

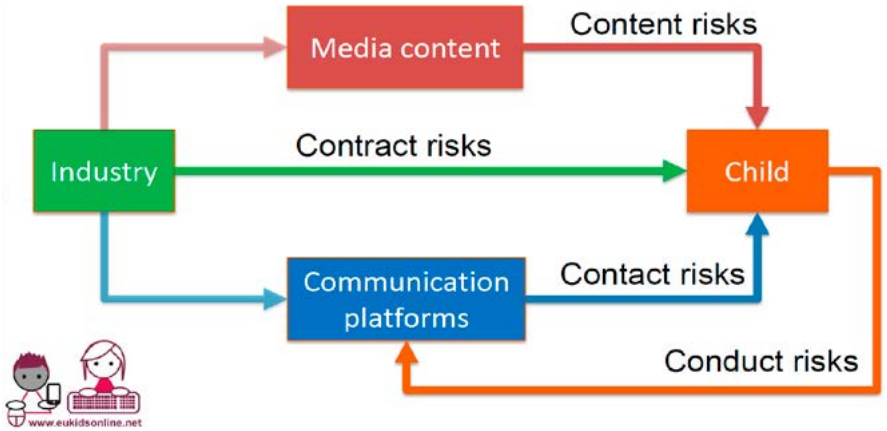
The risks of harm to children associated with use of the digital environment have been classified into 4 C's by the EU Kids Online network[51] as:

- Content risks: the child is a recipient of pre-produced media content and can be negatively affected by this – for example, pornography, violent imagery, racist content
- Contact risks: children can find themselves participating in (usually) adult-initiated interactions which put them at risk – for example, grooming, harassment, exploitation
- Conduct risks: children participate in (as agents or victims or both, since these groups can overlap) of (usually) peer-to-peer interactions which can prove harmful – for example, cyberbullying, online reputational attacks, incitement to self-harm, phishing, hacking and fraud

51. See "What are you concerned about?", Hans-Bredow-Institute (D), 2018.

- Contract risks: children can find themselves agreeing to contracts they don't understand (because they are age-inappropriate or because of the design of the site or content[52]) and which are commercially exploitative or unduly persuasive, or they may gain access online to age-inappropriate goods or services (knives, drugs, gambling, etc.)

Classification of online risks of harm to children - the 4C's from the EU Kids Online network



Additionally, the Guidelines (para 51) recognise health risks (mental and physical, including sleep deprivation, obesity, social alienation and excessive internet use).

Among these risks of harm, some are illegal, and some are legal, depending on the jurisdiction. With regard to certain risks, such as sexting, the existing legal framework might be ambiguous and not fit for purpose to address behaviour that might be part and parcel of the normal discovery of sexuality in the course of human development.[53] Revising national legal frameworks to ensure that legitimate behaviour is not criminalised might be necessary. Also, in cases of violence or abuse by children, for instance in cases of cyberbullying, frameworks might need to be revised in order to pursue suitable and adequate preventive and restorative approaches, while preventing the criminalisation of children. In many countries cyberbullying may engage the criminal law in the context of offences against the person although it is likely to be the case that involving law enforcement, or the courts will only be appropriate in the rarest of cases.

52. See Study on the impact of marketing through social media, online games and mobile applicatons on children's behaiviour (EU, 2016).
53. See Lanzarote Committee, Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, 2019.

Due to developments in relation to the digital environment more children have been exposed to the risk of sale and sexual exploitation.[54] When it comes to the prevention of sexual exploitation of children and young people, the State must provide for the protection of children and young people by adopting or strengthening, implementing and disseminating "laws, administrative measures, social policies and programmes to prevent the offences referred to in the present Protocol" (see article 9(1) of the Optional Protocol to the UNCRC on the sale of children, child prostitution and child pornography). However, the Optional Protocol also provides (in article 9(2)), that:

> *"States Parties shall promote awareness in the public at large, including children, through information by all appropriate means, education and training, about the preventive measures and harmful effects of the offences referred to in the present Protocol. In fulfilling their obligations under this article, States Parties shall encourage the participation of the community and, in particular, children and child victims, in such information and education and training programmes, including at the international level." [Emphasis added]*

There is arguably a need for greater 'participation' by children and young people in the policy-making process in this area. The child's right to information (enshrined in article 17 UNCRC) includes a right of access to appropriate information on sexual matters (sexual health, sexual offences, etc.). This is particularly true in the case of older children. In 2015, the Special Rapporteur on the sale of children, child prostitution and child pornography issued a report containing a thematic study on the issue of information and communication technologies and the sale and sexual exploitation of children, and including a section entitled "Empowering Children" in which the provision of information and the opportunity to participate (actively and meaningfully) are recognised as important within an overall focus on protection. This has again been emphasised in the UNCRC Committee's 2019 Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

Questions / Checklist for member States

- Do you promote and provide incentives to business enterprises to implement safety and privacy by design and by default as guiding principles for products and services' features and functionalities addressed to or used by children?
- Where the development, production and regular update by business enterprises of parental controls to mitigate risks for children in the digital environment is encouraged, are such controls developed and deployed taking into account children's evolving capacities without reinforcing discriminatory attitudes, infringe children's right to privacy and data protection or deny children the right to information, in accordance with their age and maturity?
- Due to the limited benefits with respect to their particular physical, psychological, social and stimulation needs are measures and policies adopted to protect infants from premature exposure to the digital environment?

54. United Nations, Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 2019.

- Is the use of effective systems of age-verification required to ensure children are protected from products, services and content in the digital environment which are legally restricted with reference to specific ages, using methods that are consistent with the principles of data minimisation?
- Are there measures in place to ensure that children are protected from commercial exploitation in the digital environment, including exposure to age-inappropriate forms of advertising and marketing? Is it ensured that business enterprises do not engage in unfair commercial practices towards children (for instance, by including misleading information about in-app purchases), requiring that digital advertising and marketing towards children is clearly distinguishable to them as such, and requiring all relevant stakeholders to limit the processing of children's personal data for commercial purposes?
- Is there co-operation with the media, with due respect for media freedom, with educational institutions and other relevant stakeholders, to develop awareness-raising programmes aimed at protecting children from harmful content as well as preventing their involvement in illegal online activities?
- Are there measures in place to encourage business enterprises and other relevant stakeholders to develop and implement policies that address cyberbullying, harassment and incitement to hatred and violence in the digital environment? Do such policies contain clear information on unacceptable behaviour, reporting mechanisms and meaningful support for children involved in such acts?
- Are good practices on ways to address risks in the digital environment shared, in relation to both prevention and remedies?
- Are public awareness-raising measures put in place about counselling, reporting and complaint mechanisms?
- Is policing with respect to child sexual abuse material victim-focused with the highest priority being given to identifying, locating, protecting and providing rehabilitative services to the child depicted in such materials?
- Is there continuous monitoring of whether and how child sexual abuse materials are hosted within your jurisdiction and are law-enforcement authorities required to establish databases of "hashes", with a view to expediting actions to identify and locate children subjected to sexual exploitation or abuse, removing or restricting access to such content and apprehending perpetrators?

Hashes

Hashes are a unique digital fingerprint assigned to digital files, including those that represent child sexual abuse material. Hashes enable the rapid analysis of large quantities of data, obviating the need to examine potential images of child sexual abuse individually. Hashes do not represent the image itself and cannot be reverse engineered to create child sexual abuse images.

- Do you engage with business enterprises to provide assistance, including as appropriate technical support and equipment, to law-enforcement authorities to support the identification of perpetrators of crimes against children and collect evidence required for criminal proceedings?

- Being mindful of available technologies and without prejudice to the principles of liability of internet intermediaries and their exemption from general monitoring obligations, do you require business enterprises to take reasonable, proportionate and effective measures to ensure that their networks or online services are not misused for criminal or other unlawful purposes in ways which may harm children, for example in relation to the production, distribution, provision of access to, advertising of or storage of child sexual abuse material or other forms of online child abuse?
- Do you require relevant business enterprises to apply hash lists with a view to ensuring that their networks are not being misused to store or distribute child sexual abuse images?
- Do you require that business enterprises and other relevant stakeholders promptly take all necessary steps to secure the availability of metadata concerning any child sexual exploitation and abuse material found on local servers, make them available to law-enforcement authorities, remove these materials and, pending their removal, restrict access to such materials found on servers outside of their jurisdiction?
- Do you participate in the annual Safer Internet Day, the European Media Literacy Week, the Council of Europe Data Protection Day, the European Day to protect children from sexual exploitation, the All Digital Week and other events organised to promote awareness among the public?

What are the Luxembourg Guidelines?

Although several conventions and other legislative instruments use notions such as 'child pornography', this has become contested over the past few years. Several stakeholders came to the conclusion that a common understanding, conceptualisation, definition, and translation of sexual exploitation and sexual abuse of children was needed, as this is important in the global effort to eradicate this type of children's rights violations. Inconsistent use and interpretation of language and terms can lead to inconsistent laws and policy responses on the same issue.

The aim was to come to a consensus on what terms to use to describe different forms of sexual exploitation and sexual abuse of children. An in-depth analysis and discussion on terminology and definitions were launched by an Inter-Agency Working Group. The IWG was chaired by Professor Jaap Doek, former Chairperson of the UN Committee on the Rights of the Child. The IWG formally concluded its work in January 2016, when the "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse" were adopted in Luxembourg.

The Luxembourg Guidelines are available at http://luxembourgguidelines.org/

A complementary reference in this context are the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography adopted by the Committee on the Rights of the Child at its 81st session in May 2019.[55]

55. Official UNCRC Guidelines (2019).

The Lanzarote Convention

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse aims to prevent and combat sexual exploitation and sexual abuse of children, whoever the perpetrator may be, to protect the rights of and provide assistance to victims, and to promote national and international cooperation in this area.

The Lanzarote Convention is underpinned by a variety of non-legally binding instruments that aim at guaranteeing that States implement effective measures against child sexual abuse, such as the Policy guidelines on integrated national strategies for the protection of children from violence.

The **Lanzarote Convention** requires States to take preventive measures, to appoint specialised authorities and co-ordinating bodies, to adopt protect measures and provide assistance to victims, to set intervention programmes or measures, to take measures to include certain offences in national criminal legislation, to ensure safeguards with regard to investigation, prosecution and procedural law, to record and store data, and to cooperate on an international level. It also installs a monitoring mechanism.

The internet is a medium that has been increasingly used for the purposes of the sexual exploitation and abuse of children, for instance to trading child sexual abuse material or to solicit children online.

The Lanzarote Convention requires States to criminalise this type of acts explicitly, in particular online 'child pornography' (or child sexual abuse material)[56] and online solicitation of children for sexual purposes (or grooming).

Article 20 para. 3 of the Lanzarote Convention provides parties with the possibility to reserve the right **not** to criminalise the production and possession of pornographic material involving children who have reached the (national) age of sexual consent, where these images are produced and possessed by them with their **consent** and solely for their **own private use**. This provision gives member States the option to exclude practices such as sexting from the criminalisation of child sexual abuse material.

The Lanzarote Committee's second round of monitoring focuses on 'The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)'. More information about the results of that monitoring round are available at https://www.coe.int/en/web/children/2nd-monitoring-round.[57]

The Model National Response

Launched in 2015 the **Model National Response**[58] grew out of the work of the **WePROTECT Global Alliance**. The Model presents a detailed framework specifically addressing online child sexual exploitation and abuse. The detailed suggestions and advice align closely with the corresponding sections of the Council of Europe's Recommendation.

56. Note that article 9 of the Cybercrime Convention also concerns offences related to child pornography.
57. See: IMEC guidance on Framing Implementation (2017).
58. See: WeProtect Model National Response.

'The Model will enable a country – regardless of its starting point – to identify any gaps in capabilities and commence planning to fill those gaps. Using the Model can assist countries in identifying actions that contribute to the delivery of the United Nations Sustainable Development Goal targets, primarily 16.2 - End all forms of violence against and torture of children. It could also assist with delivery against targets 8.7 and 5.2.'

Relevant binding and non-binding instruments

Recommendation 3.6.

United Nations, Convention on the Rights of the Child (UNCRC), article 34

Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

United Nations Committee on the Rights of the Child, General Comment No. 13 describes measures to protect children against all forms of violence

Council of Europe Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)

Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197)

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) (Lanzarote Convention)

7. Remedies

A true and effective exercise of children's rights requires that remedies are available in case of a violation of these rights. Remedies must be also available if a child's right has been infringed in the digital environment. This entails the provision of available, known, accessible, affordable, and child-friendly avenues through which children, as well as their parents or legal representatives, may submit complaints and seek remedies.

Possible avenues are: civil and criminal court proceedings, complaints to ombudspersons for children, national human rights institutions and data protection authorities, or complaint mechanisms offered by companies. In the digital environment, mechanisms provided by the actors that actually have control over technical features or content that is hosted on their platforms might be especially helpful and allow for quick redress.

Questions / Checklist for member States

- Are there available, known, accessible, affordable, and child-friendly avenues in place through which children, as well as their parents or legal representatives, may submit complaints and seek remedies? Effective remedies can include, depending on the violation in question, inquiry, explanation, reply, correction, proceedings, immediate removal of unlawful content, apology, reinstatement, reconnection and compensation.

Child-friendly complaints procedures

To be child-friendly, according to the Tool (CPAT), a complaints procedure must include the following elements:

- It is safe and accessible
- Children receive information and assistance to enable them to lodge and pursue a complaint
- Information is made available in age and disability appropriate formats including leaflets, brochures, posters for schools, and dedicated websites and disseminated in locations where children are able to find them
- Follow up, referral and response mechanisms are well-established and effective and can demonstrate that changes are implemented in response to legitimate complaints
- Feedback to such complaints is communicated directly to children within a reasonable period in a manner that is adapted to their age and understanding
- Are children provided with information and advice about remedies available at domestic level in a manner adapted to their age and maturity, in a language which they can understand and which is gender and culture sensitive? Do the mechanisms and processes that are in place ensure that access to remedies is speedy and child-friendly, and provides appropriate redress to children?
- Is in all cases access to courts or judicial review of administrative remedies and other procedures available, in line with the principles set out in the Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice?
- Are children and/or their parents or legal representatives provided with non-judicial mechanisms, administrative or other means to seek remedy, such as through ombudspersons for children and other national human rights institutions and data protection authorities?
- Are all agents working on matters of children's rights in the digital environment adequately educated and trained?
- Is the availability, adequacy and effectiveness of these mechanisms for handling cases of violations or abuses of the rights of the child in the digital environment reviewed on a regular basis?
- Are policies and measures implemented to encourage business enterprises to establish their own remedial and grievance mechanisms, in line with the effectiveness criteria set out in the UN Guiding Principles on Business and Human Rights, while ensuring that these mechanisms do not impede the child's access to the State-based judicial or non-judicial mechanisms?
- Are business enterprises encouraged to provide information, which is accessible, age-appropriate and available in the language of the child about how to introduce complaints and seek redress through remedial and grievance mechanisms?
- Are business enterprises required to make available, on their platform or within their service, easily accessible ways for any person, and in particular children, to report any material or activity which causes them concern and that reports received are dealt with efficiently and within reasonable timescales?

Relevant binding and non-binding instruments

Recommendation 3.7

Optional Protocol to the Convention on the Rights of the Child on a communications procedure

European Convention on Human Rights (ETS No. 5), articles 6 and 13

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users

Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice

Chapter 4

International cooperation and coordination

1. Ratification and implementation of UN/CoE Conventions

In a fast-moving, technologically innovative, global digital environment, international organisations can play a crucial role in sharing knowledge, ensuring effective cooperation and developing a forward look. Both at the level of the United Nations and the Council of Europe, crucial binding legislative instruments exist that are related to the realisation of children's rights, including in the digital environment.

Questions / Checklist for member States

- Have you ratified and implemented the following international instruments relevant to the promotion and protection of the rights of the child in the digital environment?
  - Optional Protocol to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000)?
  - Optional Protocol to the United Nations Convention on the Rights of the Child on a communications procedure (2011)?
  - the Council of Europe Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108),
  - the Council of Europe Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189),
  - the Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197) and
  - the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201)?
- Have you formulated reservations, and / or have you lifted reservations that may impede full implementation?

2. Cooperation with other States

- Do you cooperate with other States or international/European institutions by applying relevant international and regional instruments and arrangements, to the widest extent possible, for the purpose of respecting, protecting and fulfilling the rights of the child in the digital environment?
- Is there an adequate legal basis for providing assistance?
- Are there treaties, arrangements or other mechanisms in place to enable efficient co-operation with other States?
- Do you ensure that competent authorities can rapidly, constructively and effectively use clear channels or mechanisms for the effective transmission and execution of requests for information and other types of assistance?
- Are there clear and efficient processes in place for the prioritisation and timely execution of requests?
- Do you refrain from prohibiting or placing unreasonable or unduly restrictive conditions on the provision of assistance or co-operation?
- Do you support regional and international capacity-building efforts to improve policy and operational measures to respect, protect and fulfil the rights of the child in the digital environment, including the pooling and sharing of successful education and awareness-raising tools?
- Do you co-operate with a view to promoting standardisation of content classification and advisory labels among countries and across stakeholder groups to define what is appropriate and what is inappropriate for children?[59]

3. Cooperation with the Council of Europe

Recommendation 4 of the Guidelines requires that member States should "*co-operate with the Council of Europe by creating, implementing and monitoring strategies and programmes that respect, protect and fulfil the rights of the child in the digital environment, and share, on a regular basis, examples of strategies, action plans, legislation and good practices related to the implementation of this recommendation*."

Related relevant instruments include:

- Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users
- Internet governance Council of Europe strategy 2016-2019, Democracy, human rights and the rule of law in the digital world
- Council of Europe report DGI(2017)09, Information Disorder: Toward an interdisciplinary framework for research and policy making
- Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership
- Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries

59. For example, see the work of PEGI (Pan European Game Information).

- Work of the Council of Europe on Artificial Intelligence, including Concept note: Governing the Game Changer Impacts of artificial intelligence development on human rights, democracy and the rule of law[60] and the Recommendation CM/Rec(2020)1 of the Committee of Ministers on the human rights impacts of algorithmic systems

4. Cooperation with intergovernmental bodies, transnational networks and other international organisations

- Do you co-operate with relevant intergovernmental bodies, transnational networks and other international or European organisations?
- Can law-enforcement agencies connect to the INTERPOL database that deals with child sexual abuse material?
- Do you facilitate exchange of evidence bilaterally between jurisdictions to address child sexual exploitation or child sexual abuse material?
- Do you actively engage with the Internet Corporation for Assigned Names and Numbers (ICANN) to press for the effective implementation of policies which will enhance or sustain the rights of the child, in particular by ensuring that web addresses which self-evidently advertise or promote child sexual abuse material or any other offences against children are identified and removed, or not authorised to be registered?
- Are you keeping up to date on the latest international activities and publications aimed at guiding public policy in this area?

Relevant international organisations include (non-exhaustive list):

European

- All Digital
- BEUC
- Council of Europe
- COFACE Families Europe
- European Commission
- European Parliament
- Eurochild
- European Schoolnet
- European Data Protection Board
- ENISA
- ENOC
- Europol
- Media & Learning

United Nations

- GapMIL (Global Alliance for Partnerships on Media and Information Literacy at UNESCO)
- International Telecommunications Union (ITU)
- UNICEF
- UN Special Rapporteurs
- UNESCO

60. See: Council of Europe and Artificial Intelligence

International

- Child Dignity Alliance
- Child Helpline International
- CRIN
- ECPAT International
- ENOC
- ICANN
- IAME (International Association for Media Education)
- ICMEC
- INHOPE
- Insafe
- International Conference of Data Protection and Privacy Commissioners
- International Justice Mission
- Internet Governance Forum
- INTERPOL
- NCMEC
- OECD
- Plan International
- Save the Children International
- Terre des Hommes
- Virtual Global Taskforce
- WeProtect Global Alliance

Chapter 5

Engaging with business enterprises

The Recommendation of the Committee of Ministers on Guidelines to respect, protect and fulfil the rights of the child in the digital environment is addressed to member States. Member States have the **obligation** to secure to everyone within their jurisdiction, including children, the rights and freedoms that are laid down in international and European conventions. At the same time, business enterprises have a **responsibility** to respect these rights and freedoms. Together, States and business enterprises should aim at achieving the right balance between protecting children and ensuring equal access and opportunities of all children in the digital world. Whilst States should set clear frameworks for businesses, they should also leave room for enterprises to contribute to the fulfilment of rights.

This shared responsibility has been set out in the UN Guiding Principles on Business and Human Rights and the Council of Europe Recommendation on human rights and business, and has been clarified with regard to **children's rights** in the UN Committee on the Rights of the Child's General Comment No. 16 (2013) on State obligations regarding the impact of business on children's rights, and the Children's Rights and Business Principles developed by UNICEF, the UN Global Compact and Save the Children.

The Council of Europe Recommendation on human rights and business builds on the UN Guiding Principles on Business and Human Rights and rests on three pillars:

- States' existing obligation to respect, protect and fulfil human rights and fundamental freedoms ("the State duty to protect human rights");
- the role of business enterprises as specialised organs of society performing specialised functions, required to comply with all applicable laws and to respect human rights ("the corporate responsibility to respect human rights");
- the need for rights and obligations to be matched to appropriate and effective remedies when breached ("access to remedy").

According to the Council of Europe Committee of Ministers' Recommendation on human rights and business (2016):

> *"Member States should require that business enterprises respect the **rights of children** when operating within their territorial jurisdiction and, as appropriate, throughout their operations abroad when domiciled in their jurisdiction".*

Territorial scope

The Recommendation emphasises that business enterprises should respect the rights of children not only when they are domiciled in a member State but also when they are operating in their jurisdiction. This can be the case, for instance, if services are offered to the citizens of that member State.

Throughout the Guidelines to respect, protect and fulfil the rights of the child in the digital environment reference is made to specific measures that member States should take in relation to business enterprises. An overview of these references is provided in the following table, which illustrates the different ways in which member States' authorities should interact with business enterprises. as foreseen by the Guidelines.

States and business: different types of interaction recommended by the Guidelines

States ***require*** or ***ensure*** that businesses:
▸ Uphold and be held accountable for their human rights responsibilities
▸ Involved in developing and deploying parental controls do so taking into account children's evolving capacities and in a child rights-compliant manner
▸ Do not engage in unfair commercial practices towards children, clearly distinguish commercial advertising and limit commercial processing of children's data
▸ Take reasonable, proportionate and effective (RPE) measures to ensure their networks or services are not used for criminal or other unlawful purposes which may harm children
▸ Apply hash lists (relevant businesses)
▸ Promptly take all necessary steps to secure availability of metadata concerning child abuse material, make them available to law-enforcement authorities, remove them and, pending removal, restrict access (relevant businesses)
▸ Have easily accessible ways for reporting material or activity that causes concern, with efficient and timely receipt and handling.
▸ Undertake due diligence in relation to children's rights
▸ Perform regular child-rights risks assessments and demonstrate reasonable and proportionate measures to manage and mitigate risks
▸ Take RPE measures to ensure that their terms and conditions are enforced
States ***encourage, foster*** or ***provide incentives*** to businesses to:
▸ Co-operate with relevant stakeholders
▸ Implement safety by design, privacy by design and privacy by default as guiding principles for products, services etc. addressed to or used by children
▸ Develop and implement policies that address cyberbullying, harassment and incitement to hatred and violence in the digital environment
▸ Establish remedial and grievance mechanisms

- Provide accessible, age-appropriate information in the child's language on how to introduce complaints and seek redress
- Develop, apply and regularly review and evaluate child-oriented industry policies, standards and codes of conduct

States *engage* businesses:

- In the design, drafting, implementation and evaluation of a national strategy or action plan
- In the implementation of sectoral policies
- Through a multi-stakeholder approach, and through setting up co-operation frameworks, procedures and processes
- Like internet service providers and social network providers, to play an active role in preventing and deleting illegal content

States *help* businesses:

- To meet their responsibility to respect the rights of the child through creation of a clear and predictable legal and regulatory framework
- Through building their awareness and support regarding their roles, responsibilities and impact on children's rights and their co-operation with relevant stakeholders

(Source: Extraction of relevant references from the Guidelines, July 2020)

Inspired by the range of possible measures contained in the Guidelines, a variety of **mechanisms** can be used to engage with, support and require business enterprises to respect children's rights in the digital environment:

- Drafting a **National Action Plan on Business and Human Rights**:

The United Nations Human Rights Council has called on all member States to develop National Action Plans to support implementation of the UN Guiding principles on business and human rights.

Tools, guidance and national examples compiled by the Danish Institute for Human Rights. UNICEF also has a tool on Children's Rights in National Action Plans, with a section on children's rights and media that is particularly relevant (Section 3.7).

The Council of Europe has also invited member States to draw up such an Action Plan in its Recommendation on human rights and business, to monitor, evaluate and update the implementation of their Plan with the participation of all stakeholders and to specifically consider the rights of children in their National Action Plans.[61]

More information, for instance on NAPs, can also be found in the Council of Europe Business and Human Rights Handbook for Legal Practitioners.

61. Council of Europe (2016) Recommendation CM/Rec (2016)3 on human rights and business.

- Requiring business to businesses to undertake **child rights due diligence**, which entails that businesses should identify, prevent, and mitigate their impact on children's rights including across their business relationships and within global operations.[62] Businesses should also publicly communicate their reports on their impact on children's rights.[63]
- Promoting, facilitating and monitoring **child rights policy commitments by business companies, including impact assessments** and other **measures to support children's rights** (e.g. social investments, advocacy and public policy engagement, voluntary codes of conduct, child-rights based innovation, philanthropy and other collective actions).

UNICEF has developed a range of such tools and other relevant resources to support businesses to realise children's rights in the digital environment:

- UNICEF Toolkit for Integrating Children's Rights into Your Business
- UNICEF Child Online Safety Assessment tool (COSA)
- UNICEF Mobile Operator Child Rights Self-Impact Assessment Tool
- UNICEF ITU Industry Guidelines on Child Online Protection
- UNICEF Industry Toolkit on Children's Online Privacy and Freedom of Expression

- Setting up **channels for dialogue** with businesses such as through the organisation of roundtables or multi-stakeholder forums

Which types of business enterprises might be relevant to engage with?

- device manufacturers (such as computers / laptops, tablets, smart phones, connected toys, smart home assistants)
- Internet Service Providers
- mobile connectivity providers
- service and applications developers & providers (social media, gaming, website)
- data brokers
- cloud service providers
- analytics providers
- learning platform providers
- security providers
- financial institutions.

- Cooperating with **trade, business or industry associations**, chambers of commerce, professional training organisations, coders / engineers

62. UN Committee on the Rights of the Child (2013) General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16, para. 62.
63. UN Committee on the Rights of the Child (2013) General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16, para. 64.

Relevant associations include

- EuroISPA
- ICT Coalition
- GSMA
- ISPA
- Technology Coalition

For legal professionals of various backgrounds who seek education regarding the implementation of human rights standards, the Council of Europe HELP online courses (HELP = Human Rights Education for Legal Professionals) are very "helpful" indeed. Courses that may be relevant in the digital environment and also with regard to leading instructed co-operation with business, include, amongst others the ones on: Anti-discrimination, Business and human rights, Child-friendly justice, Data protection and privacy rights, Family law, Fight Against Racism, Xenophobia, Homophobia and Transphobia, Freedom of expression, Hate crime and hate speech, Refugee and migrant children, Right to respect for private and family life.

- Cooperating with businesses for the setting up and deploying of large-scale **awareness campaigns**

The role of the mass media

The UN General Assembly (2002) asserted that the mass media have a pivotal role to play in terms of educating and informing the general public about risk issues:

> "*The mass media and their organizations have a key role to play in raising awareness about the situation of children and the challenges facing them. They should also play a more active role in informing children, parents, families and the general public about initiatives that protect and promote the rights of children, and should also contribute to educational programmes for children. In this regard, the media should be attentive to their influence on children.*"

Today, social and online media platforms and providers also share this responsibility, since they have the scalable means to reach most if not all children and their families with awareness-raising messages.

Relevant international and regional instruments

UN Committee on the Rights of the Child (2013) General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16

UN Human Rights Council (2011) UN Guiding Principles on Business and Human Rights

Council of Europe (2016) Recommendation CM/Rec (2016)3 on human rights and business

UNICEF, Save the Children, United Nations Global Compact (2012) Children's rights and business principles

IN FOCUS: Advances in Artificial Intelligence (AI) and implications for children's rights

Two years after the adoption of the Council of Europe Guidelines, this chapter provides further insight into Artificial Intelligence (AI) and its implication for children's rights. According to a definition used at the Council of Europe, AI refers to a set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being.[64] Considering that machines only act upon human instructions and do not share the cognition of human beings, others prefer alternative definitions, for example those describing AI as "technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation".[65]

Notwithstanding the definition, it is a reality that AI is being developed and deployed in a variety of sectors and products which have the potential to touch children's lives in multi-faceted ways. From smartphones, to algorithms in social media and targeted advertising, AI is no longer a futuristic prospect, but a prominent aspect of modern life.

As with many other areas of the digital environment, AI can greatly enhance and enrich children's engagement with education, play and cultural activities. It can be used proactively to help maintain a safer online environment or to underpin different aspects of children's rights. As AI becomes more prominent it is very important to ensure children understand what AI is.

However, AI can present challenges to children's rights, including in relation to protection from discrimination. This is because AI systems operate on the basis of instructions given to them by a programmer and those instructions, in turn, will be based on data obtained from various sources. If those data reflect pre-existing biases or errors, then these will be replicated in the way AI interacts with children.[66] Moreover, as AI is fed and fuelled by significant volumes of (personal) data, concerns arise regarding intrusion on individuals' privacy and the increasing potential of highly

64. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Guidelines on Artificial Intelligence and Data Protection.
65. See definition by the British Department for Business, Energy and Industrial Strategy, used in the 2018 report "London: The AI Growth Capital of Europe" by the Mayor of London.
66. See: Report on Artificial Intelligence and Data Protection: Challenges and Possible Remedies.

personalised manipulation.[67] In its 2020 Recommendation on the human rights impacts of algorithmic systems, the Committee of Ministers referred to the impact, positive or negative, of the application of algorithmic systems with automated data collection, analytics, decision making, optimisation or machine learning capacities on the exercise, enjoyment and protection of all human rights and fundamental freedoms, and of the significant challenges, also for democratic societies and the rule of law, attached to the increasing reliance on algorithmic systems in everyday life.

Readers and users of this guide are also invited to think critically about AI in its broader context. For example, while AI systems hold great promise in many areas, this may be limited by widespread use of encryption.[68] There are currently no known forms of strong encryption that can work at scale, which will also allow smart tools to "see through the veil", and in order to identify criminal behaviour taking place through encrypted messaging and other applications.

Maximising children's rights in the context of AI will often require a balancing act, which all actors – from decision-makers and businesses, to parents, caregivers and children – must carry out. The impact of AI upon children and their rights should be taken into account at all stages of policy, law and practices in relation to children's rights in the digital environment. In other words, these considerations should be mainstreamed.

The Guidelines provide an extensive range of measures that member states should include in their national legal framework and policies regarding AI and children's rights: if implemented, these will not only help children to thrive in this era of digital revolution, big data and machine learning systems, but also ensure accountability for and protection of their rights.

Given the rapid advancement of AI, it does not seem useful to provide a comprehensive overview of the ways in which children's rights and wellbeing may be impacted. Instead, some examples of the opportunities and risks presented by AI, and according to the Guidelines' fundamental and operational principles, are presented in the table below.

Checklist / questions for member states

- Do your responses to the checklists/questions in other chapters of this handbook take account of the impact of AI upon children and children's rights?
- In particular in relation to chapter 5 (Engaging with business enterprises):
  - Are businesses required and encouraged to ensure children's rights and well-being when developing or using AI technologies?
  - Is the state engaging with businesses who develop or use AI technologies on children's rights issues and is it helping them to fulfil their responsibilities?

67. Committee of Ministers, Recommendation on the human rights impacts of algorithmic systems.
68. Converting information into a code, particularly so that it can only be understood by authorised readers.

Relevant binding and non-binding instruments

Recommendation of the Committee of Ministers on the human rights impacts of algorithmic systems (CM/Rec(20201)

Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes Decl(13/02/2019)1

Recommendation of the Committee of Ministers on measures to promote the respect to freedom of expression and information with regard to Internet Filters (CM/Rec(2008)6)

Parliamentary Assembly of the Council of Europe Recommendation 2102 (2017) on technological convergence, artificial intelligence and human rights

Useful Council of Europe resources

Council of Europe Commissioner for Human Rights (2019) Unboxing artificial intelligence: 10 steps to protect human rights, step 10 (Promotion of "AI literacy")

Council of Europe Consultative Committee of the Convention for the Protection of Individuals with Regard to automatic processing of personal data (2019) Guidelines on artificial intelligence and data protection

Frederik Zuiderveen Borgesius (Council of Europe, 2018) Discrimination, artificial intelligence and algorithmic decision-making

The Council of Europe and AI

Council of Europe (2017) Internet Literacy Handbook contains factsheets and checklists on labelling and filtering; the internet of things; artificial intelligence, automation and disruptive technologies; virtual and augmented reality; and big data, data mining and privacy (factsheets 20, 23-26). These can be used as educational sources on topics relating to AI

Relevant additional resources

UNICEF Generation AI project

Opportunities and risks related to AI in the context of children's rights in the digital environment

TYPE OF MEASURE	SPECIFIC PRINCIPLE/RIGHT	OPPORTUNITIES RELATED TO AI (EXAMPLES)	RISKS RELATED TO AI (EXAMPLES)
Fundamental principles and rights	Best interests / evolving capacities of the child	▸ AI technologies can adapt to children's maturity and capacities	▸ Children come into contact with AI technologies that are not designed with them in mind (e.g. AI devices in the home): risk of difficulty in use, exposure to inappropriate information or content
	Right to non-discrimination	▸ Empowering children with disabilities: AI can tailor products to children's individual learning, physical and other needs	▸ Bias if algorithms are designed in ways which overlook certain groups or when AI "learns" from biased or non-representative data input: risk of replicating or furthering inequalities
	Right to be heard	▸ Facilitating access to information for all children, including about their rights	▸ Law, policy and practice in relation to AI and AI technologies developed without input of children and child rights advocates, impinging on the right to be heard and overlooking their interests
	Duty to engage stakeholders	▸ Engagement with business enterprises: encourage development of AI technologies, services and policies which respect, protect and fulfil children's rights in the digital environment	▸ Lack of engagement with business enterprises: risk of development of AI technologies without consideration of the impact on children ▸ Lack of engagement with other stakeholders (parents/caregivers, civil society): risk of lack of capacity to protect and empower children in the field
Operational principles and measures	Access to the digital environment	▸ AI adaptive technologies can improve access to the digital environment, particularly for children with disabilities	▸ AI technologies may be prohibitively expensive: risk of further exclusion of certain groups of children (e.g. those in poverty, those with disabilities) in the digital environment
Operational principles and measures	Right to freedom of expression and information	▸ AI filtering systems can steer children towards appropriate online content, tailored to their interests or needs ▸ Filtering systems can block access to information disorder content	▸ AI filtering systems are automatic, usually carried out according to opaque criteria and algorithms: risk of unjustified interference with freedom of expression and information ▸ Information disorder produced through AI (e.g. "Deepfake" technology/programmes which create false or misleading stories): risk to accessing quality information ▸ Algorithms promoting non-diverse, low-quality or personalised content, based on user's viewing history and inferred interests, or content that is not age appropriate or adapted: risk to freedom to seek and receive information, freedom of thought, right to development

TYPE OF MEASURE	SPECIFIC PRINCIPLE/RIGHT	OPPORTUNITIES RELATED TO AI (EXAMPLES)	RISKS RELATED TO AI (EXAMPLES)
Operational principles and measures	Participation, right to engage in play and right to assembly and association	► AI in interactive toys and other devices can personalise and enhance children's play experience, assist in development of social skills, non-formal education (e.g. "coding toys") or development of healthy habits	► AI toys and other devices can store various types of children's data: data protection and security (hacking) risks, ethical questions of whether businesses have a duty to report and share collected data which raises issues about a child's safety ► AI toys and other devices connected to the internet: risk of being hacked and "controlled" by an external actor ► AI toys and other devices may enable location detection and tracking, surveillance of the child, by parents/caregivers and business enterprises: risk of breach of privacy and data protection ► AI devices which enable commands/orders: possible negative effect on children's development, behaviours and attitudes, particularly if devices have predominantly "female" characters
	Privacy and data protection	► Privacy automation (i.e. automatic enforcement of data privacy through computer systems) may contribute to or even enhance protection of privacy and data online	► AI devices collect and store children's data, risk to privacy and data protection rights if processing activities do not comply with data protection laws ► Collection and analysis of "big data", including online and in educational and medical fields: risk to children's data protection and privacy rights, right to non-discrimination, right to development ► Use of AI to profile children through automated processing of personal data for purposes which might negatively affect children (including commercial exploitation): risk to data protection rights and further protection issues (see "protection and safety")

TYPE OF MEASURE	SPECIFIC PRINCIPLE/RIGHT	OPPORTUNITIES RELATED TO AI (EXAMPLES)	RISKS RELATED TO AI (EXAMPLES)
Operational principles and measures	Right to education	▶ Adaptive learning systems tailored to children's needs and maturity ▶ Assisting early intervention programmes: AI predicts student outcomes and identifies those at risk of dropping out of school systems ▶ Enhanced learning experience: investment in AI in classrooms ▶ Increased teacher capacity: use of AI in teacher training and teaching methods ▶ AI in digital literacy initiatives/programmes ensure children are empowered and supported to safely use AI	▶ Classroom behaviour and performance monitoring: risk of breach of children's privacy and chilling effect on their ability to freely act and express themselves ▶ Collection of personal data through AI-powered educational tools: risk of data protection violations/breaches ▶ Conveying stereotyped or prejudiced information: risk of replicating/worsening inequalities ▶ Poor/lacking AI literacy and education leaves children exposed to risks and unable to take full advantage of AI
	Right to protection and safety	▶ Filtering systems can block access to abusive or illegal content ▶ AI can be used to assist identification, analysis, removal and reporting of child sexual abuse material and other forms of online sexual exploitation and abuse, as well as identification of child victims and abusers: greater potential speed and efficiency, lower exposure and emotional toll on relevant professionals	▶ Manipulation of algorithms to promote disguised/targeted forms of commercial content/advertising, or child profiling used to enable "micro-targeting" of commercial advertising ▶ Use of AI to produce highly attractive and potentially "addictive" games, apps, toys etc.: risk of over-use and development of unhealthy habits ▶ AI technologies used to carry out child sexual exploitation and abuse, including, grooming (e.g. convincing fake online profiles), production of highly realistic child sexual abuse material, which can also circumvent hash systems, simulation of scenarios of abuse (e.g. interactive "games", dolls/robots) ▶ Risk of increased difficulty in identifying victims, e.g. where "deepfake" technology is used to synthesise pre-existing images
	Remedies	▶ AI technologies may assist in collection of complaints (messaging or chatbots), complaint analysis and decision-making: potentially more efficient decision-making and quicker provision of remedies	▶ Risk of lack of complaints mechanisms/systems of redress in relation to AI services, technologies, etc. ▶ Where AI is used in complaints mechanisms: risks of unethical system design, error, opaque decision-making algorithms and criteria, affecting legitimacy and/or ability to challenge decisions

(Source: Council of Europe compilation and presentation – indicative, non-exhaustive overview, July 2020)

Since 2016, the Council of Europe has worked towards the promotion of the rights of the child in the digital environment through its Strategy for the Rights of the Child (2016-2021). A key instrument in this regard are the Guidelines to respect, protect and fulfil the rights of the child in the digital environment adopted by the Committee of Ministers as CM/Rec(2018)7 in 2018. These Guidelines have since been praised on as one of the most comprehensive sets of standards in this area. They are particularly appreciated for taking a balanced approach combining the protection of children in the digital world with the promotion of their positive rights as end users of digital technologies.

Complementing the Guidelines and their child-friendly version "Learn about your rights in the digital environment" published in May 2020, this handbook for policy makers underlines the importance for all public bodies, civil society and private stakeholders to adopt a common approach. Whether it be through national legislation or by developing strategic partnerships, the well-being of children in the digital environment needs to become a major joint concern for all stakeholders in the 21st century.

This handbook will help decision makers from a variety of backgrounds to support children by creating a digital world that truly respects, protects and fulfils the rights of the child. The handbook reminds them to regularly address newly emerging conditions and challenges, such as Artificial Intelligence, and proposes numerous resources and hands-on tools to check whether national legislation and policies are comprehensive and up-to-date.

Prems 091920

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE