

Policy guide on children and digital connectivity

JUNE 2018

JUNE 2018

Policy guide on children and digital connectivity

Policy Lab
Data, Research and Policy
United Nations Children's Fund
3 United Nations Plaza
New York, NY, 10017, USA
© United Nations Children's Fund (UNICEF)

ACKNOWLEDGEMENTS

This Policy Guide on Children and Digital Connectivity was produced by Policy Lab, Division of Data, Research and Policy (DRP), under the guidance of Laurence Chandy, Director of DRP. The Policy Guide was prepared by Jasmina Byrne, UNICEF Office of Research – Innocenti/DRP. Significant contributions to the document were made by Gabrielle Berman, UNICEF – Innocenti, Mario Viola de Azevedo Cunha, European University Institute, and John Carr, independent expert.

The following colleagues provided valuable input, comments and insights during the consultation and the review process: Cynthia McCaffrey, Christopher Fabian, Erica Kochi, James Powell, Sunita Grote – Office of Global Innovation; Hongwei Gao, Katell Le Goulven, David Anthony, Natalia Adler, Ian Thorpe, Toby Wicks, Brian Keeley, Celine Little – DRP; Cornelius Williams, Robert MacTavish, Anjan Bose, Rafael Obregon, Vidhya Ganesh, Juan Pablo Giraldo Ospino, Morgan Strecker, Patty Alleman, Stefan Swartling Peterson – Programme Division; Daniel Couture, Christian Larsson – ICTD; Paloma Escudero, Jordan Tamagni, Lisa Benenson, Penni Berns, Caroline den Dulk, Katarzyna Pawelczyk, Sonia Yeo – Division of Communication; Segolene Adam – EMOPS; Andres Franco, Patrick Geary, Amaya Gorostiaga, Bernadette Gutmann – PFP; Daniel Kardefelt Winther – Office of Research – Innocenti; Mark Engman, Sarah Jacobstein – UNICEF USA. The following UNICEF colleagues from Regional and Country Offices also provided significant contributions: Aida Oliver, Marita Perceval, Lorea Salterain, Bastiaan Van't Hoff, Jose Bergua, Ivan Donoso, Kamal Kamaledine, Jelena Perovic, Maria Jose Ravalli, Tannistha Datta, Wivina Belmonte, Emma Day, Sarah Jane Atkinson and Gerda Binder.

Copy editor

Margaret Ferry

Designer

Kathleen Edison

Photo credits

Cover	©UNICEF/UN0147163/LeMoyne
Page 4	©UNICEF/UN0139536/ Gilbertson VII
Page 8	©UNICEF/UN0143509/ Prinsloo
Page 12	©UNICEF/UNI144429/ Pirozzi
Page 16	©UNICEF/UN015601/Prinsloo
Page 20	©UNICEF/UN0144058/LeMoyne
Page 24	©UNICEF/UN026357/Gilbertson VII
Page 28	©UNICEF/UN058549/Holt
Page 31	©UNICEF/UN0215735/Viet Hung
Page 34	©UNICEF/UN0143100/LeMoyne

CONTENTS

Glossary	5
Introduction	6
Action 1: Affordable access	8
Action 2: Skills for all	12
Action 3: Protection from harm	16
Action 4: Privacy and identity	20
Action 5: Business standards	24
Action 6: Government policies	28
References	32



GLOSSARY

Algorithm: ‘a step-by-step procedure or method for solving a problem by a computer in a finite number of steps’¹ — Algorithms can automate the discovery of patterns in data sets and evaluate the probability of future events based on these discoveries.

Artificial intelligence: ‘a technology that appears to emulate human performance, typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogue with people, enhancing human cognitive performance or replacing people in execution of non-routine tasks’²

Biometrics: the measurement of physiological characteristics such as fingerprints, iris patterns or facial features that can be used to identify an individual³

Blockchain: a technology that allows the creation of a robust, secure, transparent and distributed value recording and transfer system⁴

Data anonymization: the process of de-identifying sensitive data while preserving its format and data type⁵

Dark web: refers to encrypted online content that is not indexed on conventional search engines. It is part of “deep web,” a wider collection of content that doesn’t appear through regular internet browsing. The dark web holds anonymous message boards, online markets for drugs, exchanges of child abuse images and more.⁶

Data governance (DG): the overall management of the availability, usability, integrity and security of data used in an organization or company⁷

Digital Citizenship: ‘the norms of appropriate, responsible behaviour with regard to technology use’⁸

Internet of Things (IoT): a computing concept that describes the idea of everyday physical objects being connected to the Internet and being able to identify themselves to other devices⁹

Privacy by default: ‘Intrinsically designing privacy into all innovations before information management capabilities are added’¹⁰

Privacy by design: ‘a multifaceted concept involving various technological and organisational components, which implement privacy and data protection principles in systems and services’¹¹

Virtual reality: ‘refers to computer-generated environments or realities that are designed to simulate a person’s physical presence in a specific environment that is designed to feel real.’¹²

INTRODUCTION

Digital technology and connectivity are fundamentally changing children's lives. As connectivity spreads to all parts of the globe and the use and application of technology widens, the impact on children and their lives grows. Children who are connected can benefit from numerous opportunities, but may also be exposed to a myriad of risks. Those who are not connected risk exclusion and disadvantage as most of the modern world remains out of their reach. The advance of new technology, such as artificial intelligence (AI), which powers critical, automated decisions, will affect children's digital lives in new ways: not only by influencing what they see online (see discussion on 'fake news'), but also by enabling access to education opportunities, jobs, health insurance and other benefits. This transition toward a digital (and offline) landscape increasingly governed by AI-enabled decisions will have a tremendous impact on children.

As an advocate for children, UNICEF is compelled to engage on this issue and work with its partners to support development of a range of policies and programmes, both to enhance children's engagement with the internet and to help make their use of it safer. As this policy guide shows, there is a recognizable inter-connectedness of policies that address access and connectivity, skills, literacies, safety and privacy. UNICEF country offices and National Committees are piloting innovative programs, supporting governments to develop national policies, conducting research on opportunities and risks online, leveraging technology for development and working with private sector partners to ensure adherence to child rights principles.

There are two motivations for this guide. First, through our work we engage with a number of stakeholders (governments, private sector, parliamentarians, civil society) who often have different priorities and models of work. Navigating this complex environment requires UNICEF to have a strong understanding of the challenges and policy implications, as well as a uniform position grounded in the rights of the child. The other motivation is to highlight conflicting issues where we still do not have sufficient clarity or evidence to help us devise policies that maximize child welfare and wellbeing.

Children who are connected can benefit from numerous opportunities, but may also be exposed to a myriad of risks. Those who are not connected risk exclusion and disadvantage as most of the modern world remains out of their reach.

This policy guide, developed by the Division of Data, Research and Policy, is intended for an internal UNICEF audience engaging with policymakers, businesses and other stakeholders at national, regional and global levels to help our communication and policy advocacy efforts. It can also be used by external audiences to help others understand the implications of digital connectivity for children and motivate them to join us in our advocacy. It builds on the State of the World's Children (SOWC) report from 2017, which focused on children and the digital age, as well as on research carried out by UNICEF Office of Research – Innocenti, its academic partners and UNICEF country offices.

The guide should not be viewed as a fully-fledged strategy or as a political position. Our knowledge in some areas is still not sufficient to allow us to definitively state what is best for children. It is not intended to be a best practice compendium, as evidence of what policies and programmes are effective is only just emerging. Our intention is that it will remain a living document and continuously evolve in much the same way that technologies, and our knowledge about their impact on children, are evolving.

This policy guide covers the following situations:

- When children use digital technology;
- When data is collected from children as they use technology (through social media, with the aid of artificial intelligence and machine learning, through the internet of things);
- When technology facilitates children's access to information and learning;
- When technology creates barriers to children's equitable access to vital services and opportunities; and
- When technology facilitates child abuse or exploitation, irrespective of whether children use it or not.

The guide is organised around the six key action points outlined in the State of the World's Children 2017 report and should be read in conjunction with the report. For each action point, the guide provides:

- A summary of the main considerations concerning digital connectivity for children;
- A set of key principles that have either been internationally agreed or are generally accepted in academic and other literature and are designed to stand the test of time despite the rapid innovation in technology design;
- Areas under discussion or areas where a) there is still no international consensus as the topic under discussion may be controversial; b) policy or regulation is emerging, but the impact is still unknown; or c) our understanding of potential implications is still developing. We hope that UNICEF can advance the debate in these areas through the generation of new evidence and insights;
- Some suggestions for UNICEF's policy and programme action that programme groups, Country Offices and National Committees can build on; and
- A list of key resources, both UNICEF and external ones, that UNICEF staff can draw upon.

The first two action points in this guide are related to affordable access to the internet and the skills and literacies needed to enable users to make the most of digital technology. The second two are related to safeguards that need to be put in place to protect children from harm online and to secure their privacy and data. The last two action points relate to actions required of the two main stakeholders: the private sector and governments. This does not mean that other actors, such as parents, civil society, religious institutions and children, do not have responsibility toward optimal, respectful and secure use of the internet and digital technology. However, with the rapid advancement of AI, internet of things (IoT), virtual reality (VR), augmented reality (AR), biometrics, blockchain and other technologies, a new burden falls on the private sector and governments to ensure a proper respect for children's rights in the digital age.

FEEDBACK AND FURTHER INFORMATION

We look forward to your feedback on the usefulness of this document and its practical implementation and suggestions on how to further unpack and operationalize this guide. For further information, consultation and guidance please contact:

UNICEF Division of Data, Research and Policy

Jasmina Byrne
jbyrne@unicef.org

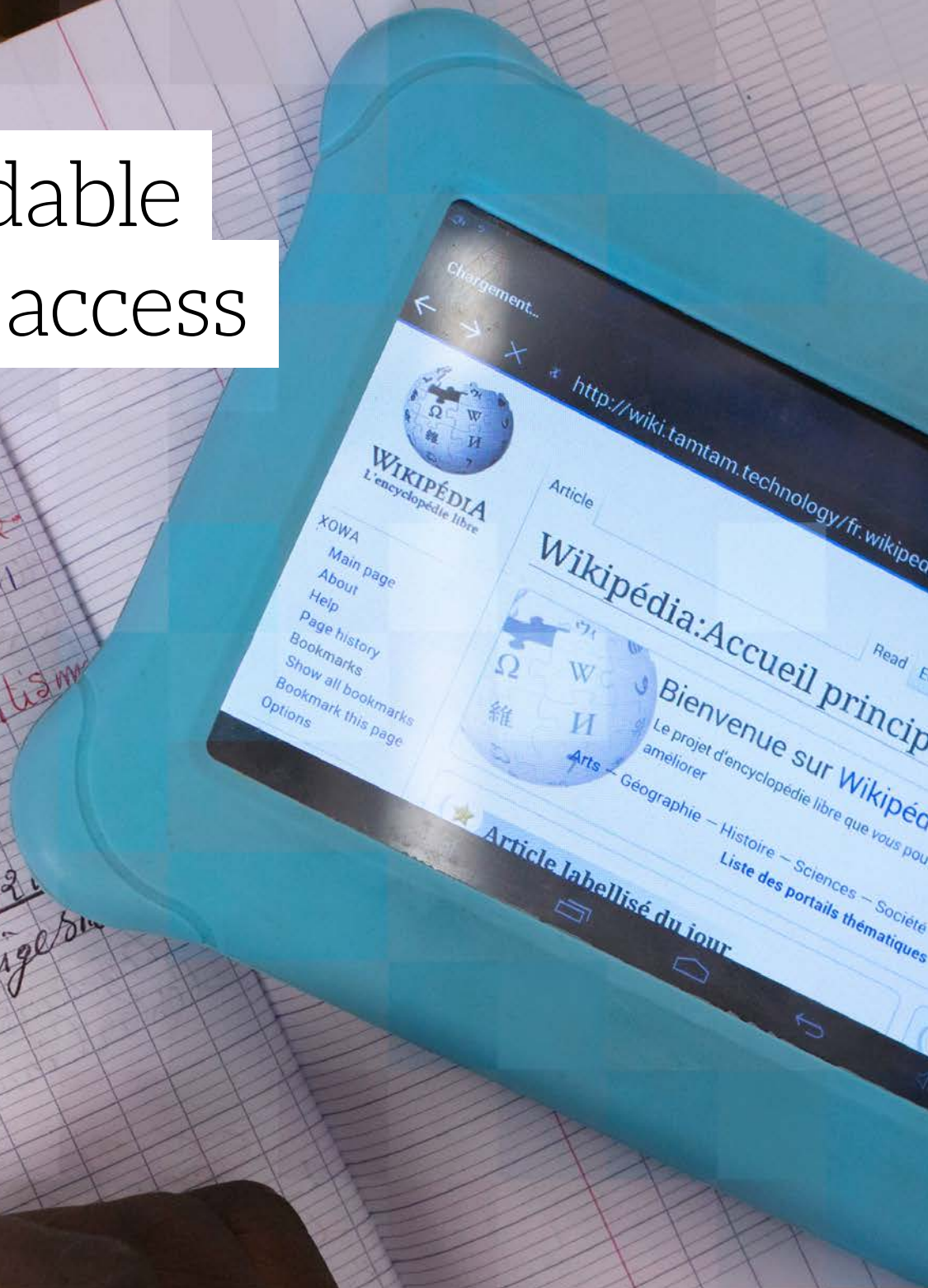
Steven Vosloo
svosloo@unicef.org

Affordable
access

maintenir
se?
maladie provoquée
dans l'organisme
ladies liées au
ntaire?
marasme, le rachitisme

Mardi, 31 Mai 1912
Observations la digestion

st une



1

All children have affordable access to high-quality online resources

Digital access is increasingly a determinant of equal opportunity for children. It enables them to benefit from access to information, educational and cultural materials, many of which are now only available online. The internet can thus be seen as a mechanism to democratize and equalize access, both to accumulated knowledge and contemporary developments, in a great many fields. A huge proportion of occupations now require some degree of technical literacy. Access to, and use of, the internet can therefore help adolescents and young people find appropriate employment opportunities. As the internet is becoming increasingly integrated into civic and political life, it provides opportunities for children and young people to engage in matters that affect them and to express their views and opinions.

Two things are essential for the provision of internet access: technological infrastructure that provides fast broadband speed, whether through wireless or mobile technologies or through networks utilising physical connections; and devices that can connect to the network in ways appropriate for the intended use (e.g., doing homework, searching for information, uploading material, communicating with friends). However, the availability of broadband network coverage, ownership of digital devices and the ability to access and benefit from the internet are quite distinct factors. There are physical barriers, such as poor infrastructure and geography. There are technological barriers, as the majority of children in lower-income countries have access only to mobile devices with low functionality, which limits their usability for complex tasks, writing or doing homework. And there are barriers related to gender and social norms, cultural practices, disability or minority status. Globally, a gender gap still persists, as the proportion of women using the internet is 12 per cent lower than the proportion of men using the internet.¹³

... the proportion of women using the internet is 12% lower than the proportion of men using the internet.

KEY PRINCIPLES

Access by child users to online resources that aid their development and education is only possible if the internet is:

- **Available and accessible for all children to use:** This includes access to devices that children can use for a range of tasks in a variety of places (schools, libraries, public places and hotspots) and with a wide range of appropriate content available in local languages and scripts.
- **Open — so as to guarantee the free flow of information and data, and based on principles of non-discrimination, freedom of expression and access to information:** The right to freedom of expression is closely linked to other rights that children may exercise online, such as participation, freedom of thought, conscience and religion, and access to information.
- **Inclusive,** as it allows children who are overlooked or excluded to benefit equally, whether they are in urban or rural environments, boys or girls, or have special needs/disabilities, and whatever their age or ethnic, religious or cultural background.



AREAS UNDER DISCUSSION

Net Neutrality: Historically, there was an accepted convention that all traffic on the internet should be treated equally or ‘neutrally’ by Internet Service Providers (ISPs). This implied that there would be no blocking, throttling, discriminating or other forms of network management which would favour one online business over another.¹⁴ This became known as the principle of net neutrality. While the issue of net neutrality is multifaceted and not always simple, it does reinforce the argument that all users all over the world should have equal access to internet content. Some zero-rating services such as Facebook’s ‘Free Basics’, enable mobile users to have free access to a limited, curated list of internet platforms or applications.

This is contrary to the principle of net neutrality and raises ethical and anti-competitive concerns by allowing children’s online access to be constrained by the commercial interests of a single company. Some see it as a pragmatic response that can help people living in less well-off countries or remote regions to obtain at least some form of internet access and valuable information. However, evidence shows that ‘Free Basics’ has not contributed in a major way to bridging the digital divide. Most of its users are not accessing the internet for the first time and are using the tool as a supplement to their existing mobile data allowance.¹⁵ Although ‘Free Basics’ is currently being withdrawn from some countries, the issue remains relevant — in principle, ISPs and platforms should not be favouring certain types of content over others based on producer, consumer or format.

Balancing freedom of expression with other rights: Some of the most fervent debates around the idea of net neutrality focus on balancing freedom of expression with other rights. For example, how to weigh easy access to harmful content for children (e.g., pornography) against the rights of other internet users to unrestricted access? How to protect the rights of children and adolescents who engage on the internet as political or social activists and who may be subject to prosecution by state and non-state actors? The question of whether internet platforms and search engines (also called intermediaries) should be under stricter regulation when it comes to issues such as hate speech, abuse, ‘fake news’, harassment and other harmful content is the subject of frequent debate. ‘Pro-regulation’ advocates say that companies cannot be arbiters of what is harmful or discriminatory, and that the internet as a public good needs to be subject to regulation. ‘No regulation’ advocates say that allowing governments to interfere will curb freedom of expression and lead to unnecessary censorship, or even worse, to deliberate interference with freedom of speech.

These debates may ultimately point the way toward new forms of trusted, hybrid institutions with the moral and legal authority to make decisions in matters of this kind. When it comes to children, the general rule should be that everything illegal or that harms the reputation of the child should be removed from the internet in line with the Convention on the Rights of the Child, which places certain restrictions on the Freedom of Expression (Article 13): *The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; or (b) For the protection of national security or of public order (ordre public), or of public health or morals.* All decisions on removal of images and texts in order to protect children’s rights and reputation must be carefully balanced against the rights of other internet users. Restrictions to combat racist, xenophobic and hate speech, discrimination and harassment should also be considered by governments and the private sector.

WHAT CAN UNICEF DO?

- **Advocate for lowering the cost of connectivity and provision of access to children in public spaces** with special attention and services for children who are disadvantaged and marginalised, e.g., girls, children with disabilities, migrant and refugee children and children in remote areas. UNICEF can track and measure disparities in access to information and communication technologies (ICTs), generate evidence to understand barriers to access and work jointly with governments and other partners to address those disparities. In addition, UNICEF should collect evidence on whether and how increased access translates into increased opportunities and better outcomes.
- **Through its engagement with the private sector, UNICEF can shape products and services to ensure increased accessibility** and influence policy and licencing frameworks in order to make these solutions scalable. (See [Principles for Digital Development](#).)
- **Invest in policies and programmes that support girls' use of ICT** through the classroom, in non-formal education environments, in communities and in their families. This would include addressing underlying cultural and gender norms that inhibit girls' access to opportunities from ICTs, particularly in societies that place less value on girls' education and empowerment.
- **Advocate for the development of age-appropriate content in local languages**, including applications and platforms that children find useful and relevant, easy to use and safe. UNICEF can partner with organizations that work with children and young people to empower them to create child-friendly apps and web content with innovative solutions to social issues and challenges. UNICEF can also support development of online platforms specifically designed for children and young people to enable them to express themselves and explore and understand their rights. (See, for example, [Voices of Youth](#).)
- **Through its work on urban policies and child-friendly city planning, UNICEF can support the development of city-wide approaches to private-public partnerships** that bring connectivity to whole neighbourhoods. Similarly, UNICEF should advocate for the expansion of high-speed internet in rural areas and universal access at low or no cost.

KEY RESOURCES

- [EU Council conclusions on digital for development](#)
- [European Convention on Human Rights \(Article 10\)](#)
- [International Covenant on Civil and Political Rights \(Article 19\)](#)
- [ITU. Girls in ICT portal](#)
- [Principles for Digital Development](#)
- [UN Convention on the Rights of the Child \(Articles 12, 13, 17\)](#)
- [UN CRC. 2014 Day of General Discussion. Digital Media and Children's Rights](#)
- [UNICEF. Discussion Paper Series: Freedom of Expression, Association, Access to Information and Participation](#)
- [UNICEF. Shaping Urbanization for Children: A Handbook on Child Responsive Urban Planning](#)
- [Voices of Youth](#) — a platform for youth bloggers
- [World Economic Forum. Internet for All](#)



Skills
for all

Skills and literacies for all children, with a focus on the underserved

Digital access provides real opportunities for children, but the availability of digital devices or provision of universal access will not necessarily produce benefits on their own. Children need to be equipped with skills and literacies to make the most of connectivity as well to understand risks and negative consequences of their internet use. They need to be able to understand their own responsibility toward other internet users in order to be good digital citizens. Digital literacy encompasses all of these areas, implying a set of competencies that goes beyond digital and technical skills. It includes the ability to: search, evaluate and manage information found online; interact, share and collaborate online; develop and create content; use safety and protection features, solve problems and be creative.¹⁶ However, not all children have equal opportunities to develop their skills and literacies.

Those in remote and underserved areas may lack access to formal education, while girls in some cultures are not permitted to use ICTs in the same measure as boys. Without sustained investment in the education sector (formal and non-formal), both in terms of introducing technology in the classroom and in the development of human capital, children may be graduating from schools unprepared for the 21st century digital market economy. Without the development of parental digital competencies, children will not be able to benefit from guidance and support in early ages.

The higher the level of digital skills and literacies, the more opportunities children will have to engage in activities that enable them to express themselves through creative use of technologies and support their active participation in civic, social and political life.¹⁷

Without sustained investment in the education sector ... children may be graduating from schools unprepared for the 21st century digital market economy.

KEY PRINCIPLES

In order to maximize the potential benefits of digital technologies, children need support to acquire skills, literacies and safety practices based on the following key principles:¹⁸

- **Safety skills — understanding risks and protecting devices, data and privacy:** Children have skills and abilities to understand the risks they may encounter online — including risks to their safety and to their privacy — so that they can use appropriate strategies to avoid risks and seek support when needed. They also need to be equipped with technical skills to protect their devices from viruses, unauthorized data access and violations of their privacy.
- **Comprehension skills — critical thinking and problem solving:** Children have skills that would allow them to search for information as well as to compare and analyse different data sources and to critically appraise information for reliability and accuracy. This includes skills that would enable children to distinguish commercial from non-commercial content.
- **Social skills — responsible communication and interaction:** Children have skills that help them communicate and interact with other internet users in a way that is positive, engaging and collaborative.
- **Curation skills — content creation and participation:** Children have skills that enable them to create and edit digital content in different formats and to express themselves through digital platforms. Through creating content (texts, images, videos) children are able to participate in discussions on issues that affect them.



AREAS UNDER DISCUSSION

Whose responsibility is 'fake news'? A 2016 study from Pew Research found that 62 per cent of adults get their news on social media.¹⁹ Children, too, access information and news from a variety of social media sites and platforms. But how confident are they that what they encounter online is not misinformation or deliberate disinformation, or so-called 'fake news'? According to the Global Kids Online²⁰ study, between 20 and 40 per cent of children between the ages of 9 and 11 'find it easy to check if the information [they] find online is true.' The emergence of so-called 'filter bubbles' occurring when platforms and search engines make use of algorithms to select information a user would want to see²¹ underlines the potential seriousness of this issue with respect to children. Instead of exposing children to a variety of ideas, different perspectives and ways of thinking, web platforms in general, and 'fake news' in particular, may lead to their engagement with news or information sources that confirm existing points of view or prejudices.

Many of the early, idealistic hopes that the internet could be a force for good, helping to bring people closer together, are now being threatened by the 'fake news' phenomenon. Who then has the responsibility to make sure that children, when accessing online resources, encounter and use only verified information from a variety of sources? Parents, as they have the responsibility to teach their children morals and values at home? Teachers, as they have the responsibility to teach children the facts and how to access and use them? Children, as they need to be able to exercise critical judgement on what they read? Or news agencies, publishers, providers of information and knowledge content, including online sources of information? Most likely, all of those actors have a role to play. The availability of false information on the internet on a huge scale certainly underlines the importance of media literacy for children. It equally constitutes a major challenge to internet businesses and platforms.

WHAT CAN UNICEF DO?

UNICEF's approach to digital literacy should focus on the promotion of the agency of children as digital citizens. Concretely, UNICEF should:

- **Develop understanding of what digital literacy means and what it encompasses,** taking into account the vastly different contexts in which we work. UNICEF should build evidence of the level of skills and literacy among children, parents and teachers so that appropriate strategies are developed to support children and those responsible for nurturing and guiding children's online use.
- **Advocate for inclusion of digital literacy education in schools and education curriculum, teacher training and extra curriculum activities:** These should be developed for all age groups, with particular emphasis on younger children in early primary school grades, as children are going online at younger and younger ages. UNICEF should advocate for children to be the current and future creators of the internet, recognizing that these are key education skills for the current age. This expands the understanding of digital literacy to proactive technical development, design and engineering thinking, which enables children to develop the technical architecture, programming and content. Digital skills should be considered an integral element when considering improvement of the education curriculum overall, so that they are taught alongside basic literacy and numeracy and other skills needed for the 21st century, such as creative and critical

thinking. In many low-income countries, underdeveloped and overstretched education systems will still place a priority on the provision of basic literacy and numeracy, so the development of digital skills will often take place in contexts other than in formal education (see below).

- **Support children from underserved or marginalized communities**, especially those boys and girls who for various social, economic and cultural reasons are not in the formal education system, to benefit from ICTs: This can include development of ICT skills in non-formal education or specialized clubs, or encouraging internet and mobile platforms to expand access and bring education to children who are currently unable to access learning opportunities.²² UNICEF should pilot and test various models to find and scale up evidence-based solutions.
- **Support the establishment of online libraries and other educational resources where children can access knowledge sources remotely and for free** (digital books, textbooks and videos) and expand the utility of public libraries so that they become centres for connectivity, internet access, e-learning and development of skills.²³
- **Skills and literacies need to be strengthened among UNICEF staff** so that we are better able to advocate at government level on behalf of children or even to prioritize programmatic actions for children in the digital era. UNICEF can monitor the information demand in situations of information vacuum (e.g., health epidemics and other emergencies) and prevent the spread of misinformation by providing timely and accurate information to the public.
- **Partner with UNESCO, Council of Europe, European Commission and other international agencies and bodies** who have experience and resources in the field of digital and media literacy, as well as with the private sector partners who have strong interest, access and technical resources.

KEY RESOURCES

- Connect Safely. [The Parent and Educator Guide to Media Literacy and Fake News](#)
- Council of Europe. [Internet Literacy Handbook](#)
- European Commission. [Media Literacy Policies](#)
- [Microsoft open access material on digital literacy](#)
- Nordicom. [Media and Information Literacy for the Sustainable Development Goals](#)
- UNESCO. [Cracking the Code: Girls' and Women's Education in Science, Technology, Engineering and Mathematics](#)
- UNESCO. [Digital Kids Asia Pacific Initiative](#)
- UNESCO. [Media and Information Literacy Curriculum for Teachers](#)
- UNESCO. [Media and Information Literacy: Policy and Strategy Guidelines](#)
- UNICEF. Discussion Paper Series: [Access to the Internet, Education and Digital Literacy](#)

Protection from harm



Risks to children's safety and wellbeing exist offline and online. The digital age has amplified existing risks and in some cases created new ones, as every digital move can be recorded and content can reach vast audiences in a single click. Child abuse, exploitation and trafficking online are still prevalent, not only on the dark web but also on mainstream digital platforms and social media. In addition, children face a range of other online risks, including cyberbullying, hate speech, harassment and exposure to unsuitable materials such as pornographic or gambling sites.²⁴ While many children navigate these risks successfully and do not experience serious harm, for some the impact can be devastating. Whether or to what extent these risks will turn into experiences that harm a child will depend on a variety of factors, not the least of which will be their individual circumstances and vulnerabilities and the availability of support mechanisms. The international community has made significant progress in formulating policies and approaches to address the most harmful online risks, such as sexual abuse and exploitation online, and there is a much better understanding of the kinds of support that are needed for victims.²⁵ Initiatives such as the [WePROTECT Global Alliance](#) have identified what needs to be done to combat online sexual abuse of children at the levels of policy and governance, criminal justice, victim support, societal change, industry engagement and ethical and informed media reporting.

KEY PRINCIPLES

Children need to be able to participate in a safe offline and online environment; be able to benefit from safe devices, applications and platforms; and know how to use the internet in a safe way. Strategies to promote children's safety online should take into account the child's age and maturity. Younger children are likely to need a higher level of support and guidance from parents, teachers and other trusted adults.

- **Safe environment:** What makes some children vulnerable to harm from violence and abuse depends largely on their life context, their individual characteristics, family circumstances, cultural context and availability of support networks. Prevention and response efforts to tackle violence against children online therefore need to address both the physical and online environments by building a safety infrastructure aimed at children and their caregivers in the form of laws, policies, structures and support services as well as complaint and redress mechanisms. More evidence is needed on what makes certain children particularly vulnerable to harm and the interplay between offline and online risk factors.
- **Safe devices, applications and platforms:** In order to minimize situations in which children might encounter harmful behaviour and content, safety features need to be built into technological products or services from the outset. When it comes to younger children, those features could include parental controls, firewalls, and apps designed specifically for children. Other measures could include content rating and classification so that children do not have unwanted exposure to extreme violence and pornography; age verification tools; tools for reporting misuse and abuse; as well as removal and blocking of illegal content such as child abuse material. (See [European Better Internet Strategy](#).²⁶)
- **Safe use:** Children should have the skills to use digital devices and platforms in a safe way in order to avoid abuse and exploitation online, encountering inappropriate content, and engaging in activities that may be illegal or harmful to other users, such as harassment or bullying (see also section 2: Skills and Literacies). Promotion of safe use is the responsibility of all stakeholders, including parents and caregivers, educators, the industry, civil society and, increasingly with age, children themselves.



AREAS UNDER DISCUSSION

Removal, blocking or filtering? Blocking and filtering are used interchangeably to mean ‘making one part of the internet inaccessible to the user’, while removal usually refers to the full exclusion of illegal content from the source. Governments all over the world are increasingly calling for the removal from the internet of material that is illegal within their jurisdiction.²⁷ In addition, policy makers may call for service providers to restrict access to certain kinds of services or content. Online gambling, for example, is either illegal in many jurisdictions or it is limited by law to adults. Child protection and national security concerns can also give rise to measures that restrict access to certain types of material. Other than issues relating to child sexual abuse images, there is little international consensus on what constitutes inappropriate or illegal content. Governments are thus increasingly taking steps at a national level to ensure that what is illegal offline is also illegal online.²⁸

Some argue that blocking or restricting access may have negative implications, as it does not deal with the underlying problem, it is easy to circumvent and mistakes could easily be made that would lead to legitimate content becoming inaccessible.²⁹ Blocking should be undertaken with caution so as to ensure it does not interfere with other rights of children, including access to crucial information. There are many examples of schools being overzealous with filtering content in order to protect children, beyond what is prescribed by law, thus blocking access to sites that may be valuable to children (for example sex education material). (See, for example, [Children’s Internet Protection Act](#).³⁰)

‘How much time online is harmful for children?’ is a question that bothers many parents, educators and even children. We still do not know enough about how time spent online impacts children’s wellbeing in the long run, including what other opportunities it may crowd out.³¹ As with most things, it is likely that use in moderation is best. The question that parents need to ask is not how many hours children spend in front of their screens, but what they spend their time on (reading, studying, playing games or talking to friends) and whether that takes too much time away from sleeping, playing and being physically active.³²

Despite lack of good evidence, some attempts have been made to regulate the time children spend online. In 1999, the American Academy of Pediatrics (AAP) recommended no screen time for children younger than 2 and only two hours per day for older children. These guidelines were revised in 2016 to reflect the realities of modern life. There is now less emphasis on time use and more emphasis on the content children encounter online and the value of using technology along with parents.

In another attempt to curb screen time, South Korea enacted a law in 2011 that made it illegal for children under the age of 16 to play online games between midnight and 6:00 a.m. The law was not very effective, as it led to an increase of only 1.5 minutes of sleep duration per night.³³ Other ways to prevent children’s possible overuse may prove more helpful, but before we have adequate evidence to inform policy and practice, it may be prudent to avoid blanket recommendations and overly restrictive interventions.

WHAT CAN UNICEF DO?

- **Continue building an evidence base on what makes children particularly vulnerable to violence, abuse and exploitation offline and online** and understanding the prevalence and factors that underline such occurrences as well as the interplay between risk, vulnerability and harm.³⁴

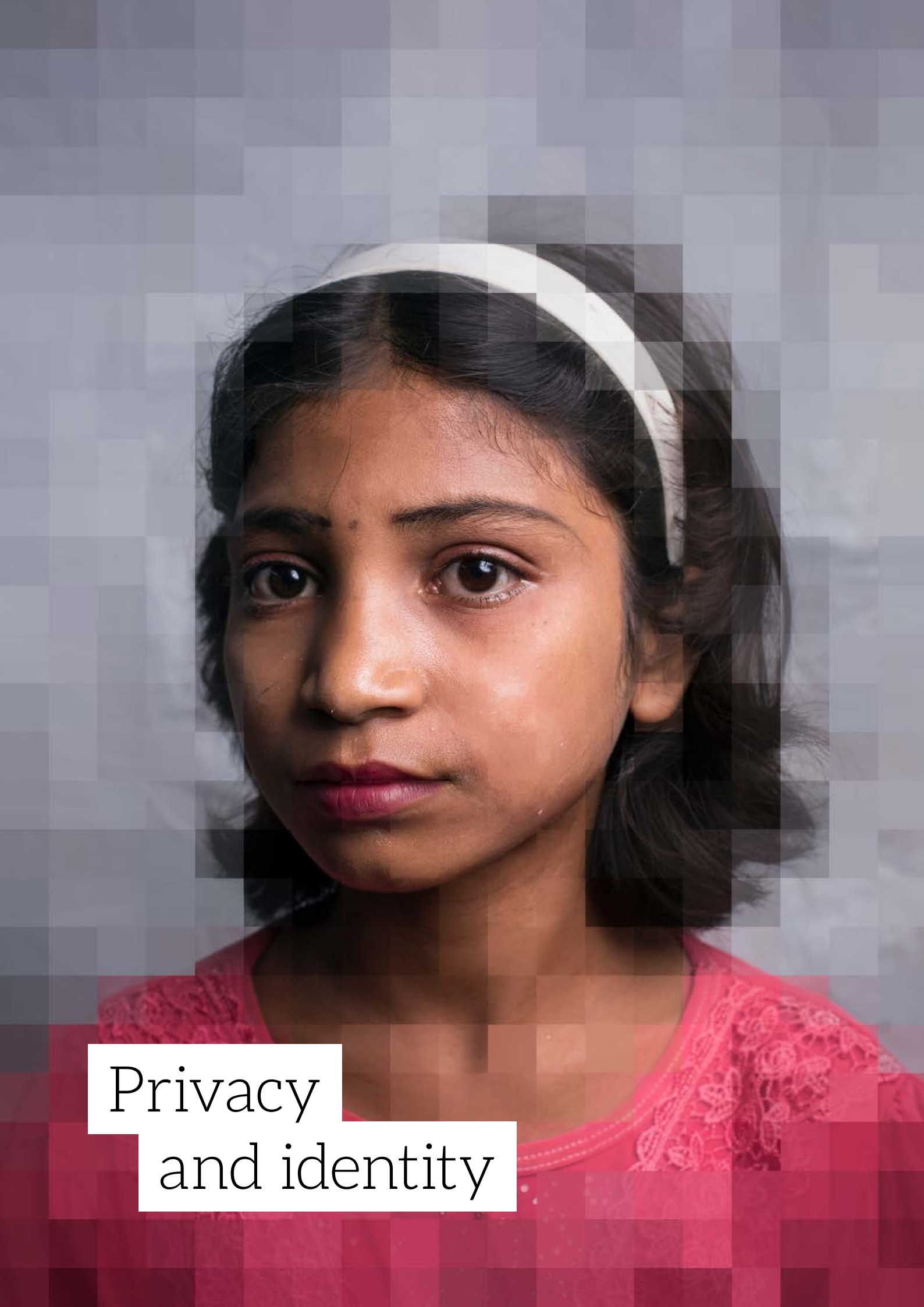
- **Support national efforts to develop comprehensive child safety online policies and strategies** that are aligned with national plans and strategies to combat violence against children. This should include advocating for more countries, organizations and entities to join WePROTECT Global Alliance, a concerted international effort to combat child sexual abuse online. The WePROTECT Global Alliance [Model National Response](#) is an excellent framework that can be contextualized for countries with limited regulatory capabilities. Using this model, countries can assess their current response, identify gaps and establish priorities in efforts to address them.
- **Given its recognized global leadership in child protection, UNICEF should work with its government and private sector partners to define a comprehensive agenda** to address online risks, vulnerability and harm, including newly recognized risks to child wellbeing such as excessive use of the internet, harassment, hate speech and discrimination. This should include both preventative action through awareness raising, training and vulnerability assessments, as well as support for victims, including helplines, counselling and remedial measures.
- **UNICEF should provide technical guides, best practice models and other resources to national partners** and develop knowledge exchange mechanisms that foster South-South and horizontal collaboration and learning on child safety online.

KEY RESOURCES

- [Children's Charities' Coalition on Internet Safety](#)
- [Council of Europe Guidelines to promote, protect and fulfil children's rights in the digital environment](#)
- [European Commission Communication on Tackling Illegal Content Online](#)
- GSMA. [Internet Safety Guides](#) (cover cyberbullying, discrimination and hate speech online, grooming, illegal content, inappropriate content, privacy, sexual extortion of children, sexual harassment online, and unsolicited contact from strangers)
- GSMA. [Safety, privacy and security across the mobile ecosystem](#)
- [International Telecommunication Union Child Online Protection](#)
- [Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography](#)
- The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (also known as [Lanzarote Convention](#))
- [UK Internet Safety Strategy](#)
- [WePROTECT Global Alliance Model National Response Guidance Document](#)
- WHO. INSPIRE: [Seven Strategies for Ending Violence against Children](#)

UNICEF RESEARCH AND REPORTS

- UNICEF EAPRO. [Child protection in the digital age](#)
- UNICEF India. [Child Online Protection in India](#)
- UNICEF MENA. [Child Online Protection](#)
- UNICEF Office of Research – Innocenti. [Global Kids Online Research Synthesis 2015-2016](#)
- UNICEF ROSA. [Victims are not Virtual](#)



Privacy
and identity

Safeguarding children's privacy and identity online

The right to privacy is a fundamental human right. Privacy is essential for the development of a child's personality, identity and autonomy, while the violation of the right to privacy might affect other human rights, including the right to freedom of expression and to hold opinions without interference.³⁵ In the digital age this right has gained a new meaning and a new, higher level of significance.

Privacy is no longer related solely to the physical environment. As modern communication practices involve using one or many internet-based platforms, and as children are leaving longer and wider trails of digital information, their data can easily shift from private to public. Data generated through internet browsing and use of social media can be used for inappropriate advertising and marketing, profiling and surveillance by government and others. Various devices connected to the internet (toys, home appliances, personal assistants) can transmit data collected even from very young children to servers where security standards may be lax and open to hackers. Similarly, online data collected by both government and the private sector may be susceptible to cyber-security attacks and/or be vulnerable to misuse by authoritarian regimes.

Children, especially the younger ones, often do not have the necessary skills or a full understanding of the risks associated with using digital media...

Technology holds great potential to address issues of identity and to help overcome challenges related to lack of birth registration and certificates. Children also seek to form informal identities online through use of social media platforms. While it is important to incentivize the development of solutions that can increase access to formal and new, less formal forms of identity, it is necessary to ensure that data collected for such purposes is stored and used in a way that does not breach individual privacy and personal security.

Children, especially the younger ones, often do not have the necessary skills or a full understanding of the risks associated with using digital media, or the loss of control over content, and how, once it has appeared online, it can follow them into adulthood. Irrespective of whether children wish to and are able to closely guard their privacy online, they should have at their disposal all the opportunities, information, tools and safety measures to do so.

KEY PRINCIPLES

Respect for children's privacy and identity and protection of their data requires concerted action and commitment by all stakeholders, including international organizations such as UNICEF. It requires proactive, preventative and protective measures.³⁶

- **Proactive:** A clear commitment and consensus by all stakeholders to respect and enforce high standards of privacy for children and protection of their data, even when laws and regulations have not yet caught up with various privacy concerns.
- **Preventative:** Such measures address privacy and data protection violations before they happen. They can include either privacy by default, where the privacy settings of any device and technology are automatically set by default, or privacy by design, embedded into the design of business processes, technologies, operations and information architectures in a holistic, integrative and creative way.³⁷ Methodologies that embed privacy in the design of services and applications are also referred to as Privacy Enhancing Technologies (PETs).

- **Protective:** Where personally identifiable data from children is processed for legitimate reasons and with properly obtained consent, their privacy must be continuously protected across the entire life-cycle of the personal data: from data creation and collection, through its use, storage and processing, to its destruction. This includes the right to have personal data erased — the ‘right to be forgotten’ — which is especially important for children as they navigate their path through childhood and forge digital identities along the way. Under EU General Data Protection Regulation (Article 17), everyone, including children, is entitled to have data they posted online as a child erased without establishing a specific reason. Protective measures and safeguards need to be based on international standards and best practices and aim to balance protection of children’s data and privacy against other rights. Concurrently, data collected should be limited only to that which is necessary for the specific purpose (i.e., data minimization) and balanced against the potential risk such data collection can have for the child, including risks of interception from governments and others with broad surveillance powers (i.e., proportionality).



AREA UNDER DISCUSSION

Privacy and data protection in times of artificial intelligence and machine learning: The sheer amount of data collected and processed by algorithms and other forms of artificial intelligence poses fresh challenges to privacy. Companies are using artificial intelligence in the development of new products and services, often embedded in internet-enabled devices. Data collected from users is a valuable commodity that enables revenues from marketing and advertising. Governments are using AI to build smart cities, customize education, improve transportation, and to strengthen national security and law enforcement. These advancements have implications for several policy areas, including privacy and data protection.

Many questions remain, as legal frameworks in many parts of the world have not yet caught up with this rapidly evolving field. For example, shouldn’t data anonymization be embedded in the design of technologies? To what extent can data encryption safeguard users’ information and preserve the best interest of the child? How can the concepts of consent and ownership be operationalized? What policies and tools are required to allow for monitoring and audits of algorithms and, more generally, AI systems and institutions and the data they use? What should data governance systems entail?³⁸

Within the EU, certain forms of data collection and processing for commercial purposes with respect to children’s data became illegal in May 2018, when the General Data Protection Regulation entered into force. A variety of technical measures are also becoming available that can help protect or anonymize children’s data.

WHAT CAN UNICEF DO?

- **Develop a better understanding of what children consider private in the digital age** by conducting research and consultations with children about their perceptions and understanding of risks of loss of privacy.
- **Advocate for stronger protection of privacy rights for children with governments, the private sector, education institutions and parents:** UNICEF should in particular encourage social media platforms and other mobile and internet services, products and

applications to simplify terms and conditions and privacy policies that children can easily understand, and provide them with easy ways to report breaches of privacy. UNICEF should encourage businesses not to use children's personal data for the purpose of marketing or creation of user profiles for targeted advertising.

- **UNICEF should examine the privacy implications in its own projects that use digital technologies to collect, store, share or analyse children's data** and design appropriate strategies to mitigate against potential violations of their right to privacy. (See, for example, [UNICEF Procedure for Ethical Standards in Research, Evaluation and Data Collection and Analysis](#).)
- **Encourage transparency and accountability (including for algorithms) wherever possible when using children's digital data for decision-making** on matters that directly affect them. UNICEF can play a key role in advocating for policies and best practices that work toward the equitable distribution of AI's benefits, and protection of children's fundamental rights by working toward preventing discriminatory outcomes in AI.

KEY RESOURCES

- [European Union General Data Protection Regulation](#)
- [Girl Effect. Digital Safeguarding Tips and Guidance](#)
- [Information and Privacy Commissioner Office, Ontario. The 7 Foundational Principles of Privacy by Design](#)
- [UNICEF Office of Research – Innocenti. Child Privacy in the Age of Web 2.0 and 3.0](#)
- [UNICEF Office of Research – Innocenti. Ethical Considerations When Using Social Media for Evidence Generation](#)
- [UNICEF. Children and Digital Marketing: Rights, Risks and Responsibilities](#)
- [UNICEF. Discussion Paper Series: Privacy, Protection of Personal Information and Reputation](#)
- [UNICEF. Industry Toolkit: Children's Online Privacy and Freedom of Expression](#)
- [United Nations General Assembly Resolution The Right to Privacy in the Digital Age](#)
- [World Economic Forum. How to Prevent Discriminatory Outcomes in Machine Learning](#)

Business standards



The private sector has been the main driver of the technological revolution. It exercises three main roles in our digital lives, as provider of internet access, provider of content and other digital goods and as online retailer.³⁹ Some private sector entities may play more than one of these roles. As gatekeepers that control the flow of information across the network, they can have access to vast amounts of children's information and data. In these roles, they can have great power and influence over children's lives and their rights. But this also means they have heightened responsibility.

[The private sector has] great power and influence over children's lives and their rights. But this also means they have heightened responsibility.

Businesses can enable the fulfilment of children's rights by: providing connectivity; facilitating access to knowledge, services and goods; working with governments to take down child abuse material or other inappropriate content; protecting children's privacy; and raising awareness of safe and responsible internet use. The private sector has a key role to play when it comes to maintaining users' trust in the internet by developing ethical standards and approaches to technological design and business practices. There has to be a universal commitment to minimum ethical standards to which business must adhere, irrespective of the country in which they operate.

KEY PRINCIPLES

- **Commitment:** Businesses should demonstrate a clear policy commitment to respect children's rights as described in key international guidelines (see below). This policy commitment should stipulate expectations of all those involved in operations and services and include ethical standards, codes of conduct or other values-related corporate commitments and policies.
- **Responsibility:** Companies have a responsibility to respect child rights in the context of the digital environment, in particular the rights to non-discrimination, information, freedom of expression, privacy and protection from abuse and exploitation. For example, businesses should prevent use of their networks and services for the distribution of illegal content, including child sexual abuse images and xenophobic, racist and hate speech. They should take measures to safeguard children's privacy and facilitate children's access to beneficial information.
- **Transparency:** The private sector should publicly share efforts to address the impact of digital technologies and digital media on children's rights. For example, companies should be open about what measures they have put in place to monitor the posting of illegal and harmful material, how they respond to children's requests to take down offensive content, how they use and share data collected from children online, and the nature and extent of any filtering mechanisms to protect children from accessing harmful content. Responsible and transparent business practices contribute both to higher corporate accountability and to increased trust by the most vulnerable digital consumers: children.



AREA UNDER DISCUSSION

Responsibility or liability? In many jurisdictions, online platforms have no legal liability for any hate speech, slander, 'fake news' or other form of content that is published by third parties who use their service, providing the platform owner had no prior knowledge of the content. Perhaps because they cannot be held liable, too many companies have not yet engaged quickly or sufficiently in finding and removing illegal and offensive content, despite the fact that their policies expressly forbid such material. The prevailing order is that removal of such content happens once the company is notified by users. This can mean that harmful or illegal content remains accessible online for considerable periods of time. This type of immunity for intermediaries emerged in the early days of the internet when there was a worry that a proliferation of lawsuits might crush or severely constrain innovation by the predominantly small businesses that were then pioneering the development of new online services.

As we approach the 30th anniversary of the internet, public opinions are shifting. While it would be wrong in principle to say that a company can be liable for content or activity on its site of which it could not possibly have had any actual knowledge, it has to be recognized that broad-ranging immunity may become an excuse for inaction. The Council of Europe suggests⁴⁰ that governments should require companies to take reasonable and proportionate steps to ensure that their terms and conditions of service are being met. This does not interfere with the principle of immunity, but it does place an obligation on companies to ensure that they are making efforts to provide the sort of online environment that they advertise to all members of the public, children included.

WHAT CAN UNICEF DO?

- **Influence businesses to take into account the needs of the most marginalized and excluded groups of children** in order to shape products and services in the future, so businesses can meet their obligations to those communities and child rights more broadly.
- **Carry out advocacy with mobile operators, internet companies and platforms to adopt more child-rights focused business standards and practices**, meet their responsibilities under international guidelines and adapt and implement their safeguarding policies to reflect these responsibilities: This should include prevention of distribution of child abuse images and sharing of online content that is considered illegal or harmful to children.
- **Encourage business entities and technological companies to pioneer innovative solutions** to the aforementioned problems that take into account different local contexts and culture: These could include safety designs that are embedded in technologies and services as well as the development of a range of tools that parents can use to minimize risks for their children, including password protection, age verification, block/allow lists and others.
- **Support businesses to develop ethical standards for their operations**, including for data collection and processing, marketing and advertising, and provide them with necessary resources and tools; work with business champions to advocate with and support other companies to respect and commit to the realization of child rights.
- **Work together with business partners to raise awareness about safe, responsible internet use** and build digital skills of children and their parents.

KEY RESOURCES

- [Children's Rights and Business Principles](#)
- [DeepMind Ethics & Society](#)
- [GSMA. Notice and Takedown: Company policies and practices to remove online child sexual abuse material](#)
- [UN Guiding Principles on Business and Human Rights](#)
- [UNICEF. Children Are Everyone's Business Workbook](#)
- [UNICEF. Children's Rights in Policies and Codes of Conduct](#)
- [UNICEF. Digital Marketing and Advertising](#)
- [UNICEF. Discussion Paper Series: Children's Rights and Business in the Digital World](#)
- [UNICEF. Good practices](#)
- [UNICEF. Stakeholder Engagement Guide](#)
- [UNICEF/ITU. Guidelines for Industry on Child Online Protection](#)

A close-up photograph of a woman wearing a blue hijab, looking down at a smartphone held in her hands. The lighting is dramatic, with strong highlights on her face and hands, and deep shadows elsewhere. The background is dark and out of focus.

Government policies

Inclusive, evolving and evidence-informed government policies

Information communication technologies can accelerate progress and development, contribute to the realization of human rights and help bridge economic divides. Governments are readily embracing ICTs in national policies that address different sectors of the economy and society, including through the development of strategies that address broadband access, smart societies, e-governance, cyber-security and human rights.⁴¹ Despite estimates that children account for one-third of all internet users,⁴² current international and national digital policies too frequently fail to take children's issues sufficiently into consideration.

Despite estimates that children account for one-third of all internet users, current international and national digital policies too frequently fail to take children's issues sufficiently into consideration.

Digital policies and strategies, including those that address artificial intelligence and machine learning, operate primarily through the lens of the adult user or beneficiary. At the same time, national policies that deal with children's rights and welfare, health and education have yet to acknowledge the relevance of digital connectivity for realizing these wider goals. Children's needs therefore have to be integrated in all ICT regulations and policies, the development of which should be informed by children's own views and outlooks.

KEY PRINCIPLES

Governments, international agencies and regional organizations need to ensure that all policies, laws, guidelines, standards and recommendations related to the digital environment properly integrate and take account of children's needs and their rights. Such policies should be:

- **Inclusive — as they focus on children's inclusion and equity:** Particular regard should be given to the needs of children from the most marginalized groups, and those deprived of opportunities to benefit from digital connectivity or are at heightened risk of harm. Policies need to focus on both boys and girls and be tailored to specific age groups. Such policies need to be comprehensive and consider all aspects of child welfare especially in relation to access to information and services and protection from harm. They should also be mindful of the importance of the child's right to participation in processes affecting them and their wider right to freedom of speech.
- **Evolving — as they adapt to technological and social change and address new and emerging challenges:** Given that technological innovation often outpaces the development of policy, governments and other policy makers should consider developing universal, core principles that are technologically neutral, but can be easily adapted to new realities.
- **Evidence informed — as informed by evidence on disparities in access, children's experiences in using technologies and evidence on the use of children's data:** Evidence should also be generated about effective programme models and strategies, and evidence of policy impact should be documented and disseminated to benefit other countries.



AREA UNDER DISCUSSION

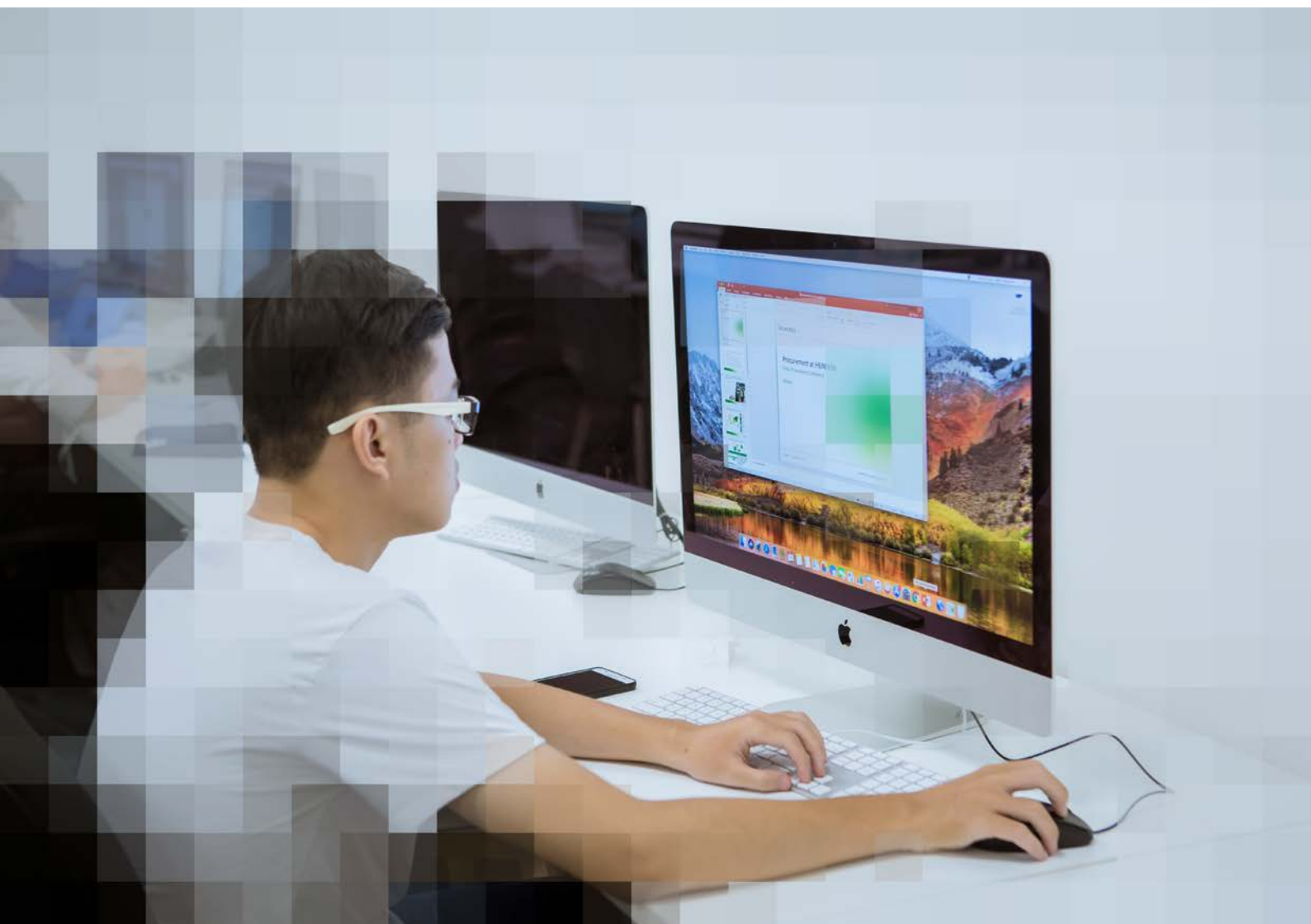
Is there a need for a new social contract? The idea of a multi-stakeholder approach to internet governance emerged in the early to mid-2000s as part of an attempt to reach a consensus or a compromise between those who believed there should be no external involvement in running the internet and those who favoured traditional governmental or inter-governmental controls.⁴³ Those stakeholders have greatly contributed to the development of 'shared principles, norms, rules, decision-making procedures and programmes that have shaped the evolution and use of the internet'.⁴⁴ This idea of a 'shared internet' is being threatened by various actors who are operating outside this framework — either as individual governments or within the private sector. Today, many internet governance issues are increasingly being decided at regional and national levels, which, some critics say, may lead to the fragmentation of the internet and policies that are not in line with internationally agreed norms. All this has led to debates about the need for a new model or approach to multi-stakeholder collaboration or a new social contract where 'each actor has the responsibility to act not only in their own interest, but in the interest of the internet ecosystem as a whole'.⁴⁵ With persistent inequalities in access and opportunities and newly emerging threats to children's safety and privacy online, some form of multi-stakeholder cooperation is not only desirable but also necessary. This collaboration not only entails collective responsibility toward creation of the safe and positive online (and offline) environment, but also our joint, societal responsibility toward child welfare and wellbeing.

WHAT CAN UNICEF DO?

- **At the national level, UNICEF should work with all relevant government departments to integrate children's issues into national digital policies and strategies.** UNICEF should also advocate for an overarching policy on children and digital connectivity that incorporates key international principles (see the list of resources) and outlines concrete, measurable steps for digital inclusion, development of skills and literacies, online safety and data protection.
- **At the international level, UNICEF should advocate for better inclusion of children's issues and their voices in internet governance forums** and in relation to ICT for sustainable development policies and strategies. UNICEF should partner with sister UN agencies (ITU, UNESCO, UN Women, UN DESA), World Economic Forum and other international organizations to forge a coalition of global advocates for children's rights.
- **UNICEF should continue to build evidence on underlying drivers of policy formulation and implementation** and document policy-making models and approaches that can be transferred across countries and regions.

KEY RESOURCES

- [BIK Map II: Policy Mapping for the European Strategy for a Better Internet for Children in European Member States](#)
- [Council of Europe Guidelines to promote, protect and fulfil children's rights in the digital environment](#)
- [Global Kids Online](#)
- [UN CRC. 2014 Day of General Discussion. Digital Media and Children's Rights](#)
- [UNICEF. State of the World's Children 2017](#)



REFERENCES

- ¹ cs-Fundamentals.com.com: Programming Tutorials and Interview Questions. <http://www.cs-fundamentals.com/tech-interview/dsa/what-is-an-algorithm.php>
- ² Gartner IT Glossary. <https://www.gartner.com/it-glossary/artificial-intelligence/>
- ³ National Institute of Standards and Technology. US Department of Commerce. <https://www.nist.gov/programs-projects/biometrics>
- ⁴ Axon, L. (2015). Privacy-awareness in blockchain-based PKI. CDT Technical Paper Series 21/15, Centre for Doctoral Training in Cyber Security. Oxford. Available at: <https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b>
- ⁵ Raghunathan, B. (2013). The Complete Book of Data Anonymization: From Planning to Implementation. Taylor & Frances Group, LLC.
- ⁶ <https://www.investopedia.com/terms/d/dark-web.asp>
- ⁷ <http://searchdatamanagement.techtarget.com/definition/data-governance>
- ⁸ UNESCO (2016). A Policy Review: Building Digital Citizenship in Asia-Pacific through Safe, Effective and Responsible Use of ICT. UNESCO. Paris. Available at: <http://unesdoc.unesco.org/images/0024/002468/246813e.pdf>, p. 14
- ⁹ Techopedia. <https://www.techopedia.com/definition/28247/internet-of-things-iot>
- ¹⁰ Cavoukian, A. and Popa, C. (2016). Embedding Privacy Into What's Next: Privacy by Design for the Internet of Things. Privacy and Big Data Institute. Ryerson University. Toronto. Available at: <https://www.ryerson.ca/content/dam/pbdce/papers/Privacy-by-Design-for-the-Internet-of-Things.pdf>
- ¹¹ European Union Agency for Network and Information Security. <https://www.enisa.europa.eu/topics/data-protection/privacy-by-design>
- ¹² <https://www.techopedia.com/definition/4784/virtual-reality>
- ¹³ ITU Facts and Figures 2017. The gender gap represents the difference between the Internet user penetration rates for males and females relative to the Internet user penetration rate for males, expressed as a percentage. <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>
- ¹⁴ Buell, M. (2017). What Net Neutrality is (and Isn't). Internet Society. Available at: <https://www.internetsociety.org/blog/2017/05/what-net-neutrality-is-and-isnt/>
- ¹⁵ Global Voices Advox (2017). Free basics in Real Life: Six case studies on Facebook's internet "on ramp" initiative from Africa, Asia and Latin America. Available at: https://advox.globalvoices.org/wp-content/uploads/2017/08/FreeBasicsinRealLife_FINALJuly27.pdf
- ¹⁶ Kranchev, P. in UNICEF (2017). State of the World's Children. Children in a Digital World, p. 38
- ¹⁷ See, for example, research from Global Kids Online www.globalkidsonline.net and EU Kids Online
- ¹⁸ There are several definitions and key principles of digital literacy — the principles in this document are derived from the European Commission and the work of Petar Kanchev, Safer Internet Programme Bulgaria, also presented in the SOWC
- ¹⁹ Gottfried, J. and Shearer, E. (2016). News Use Across Social Media Platforms 2016. Pew Research Center. Available at: <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/>
- ²⁰ Byrne, Jasmina, et al. Global Kids Online Research Synthesis: 2015-2016. UNICEF Office of Research – Innocenti and London School of Economics and Political Science. Florence. Available at: <https://www.unicef-irc.org/publications/869-global-kids-online-research-synthesis-2015-2016.html>
- ²¹ Techopedia. What does filter bubble mean? <https://www.techopedia.com/definition/28556/filter-bubble>
- ²² See, for example, Brazil case study, in UNICEF (2017). State of the World's Children, p. 15.
- ²³ See, for example, Library for All <http://www.libraryforall.org/>
- ²⁴ For further understanding of different types of online harm, see Luxembourg Guidelines: Terminology Guidelines for the Protection of children from sexual exploitation and sexual abuse http://www.ilo.org/ipecc/Informationresources/WCMS_490167/lang--en/index.htm and UNICEF. (2017) State of the World's Children. Typology of ICT Related Harms, p. 73.

²⁵ See, for example, WePROTECT Protect Global Alliance Model National Response, available at: <http://www.weproTECT.org/the-model-national-response/>

²⁶ European Commission Communication COM(2012) 196 final: European Strategy for a Better Internet for Children. Brussels 2/5/2012. Available at: <https://ec.europa.eu/digital-single-market/en/news/communication-european-strategy-make-internet-better-place-kids>

²⁷ See, for example, EC Communication COM(2017)555 on Tackling Illegal Content Online – Towards an enhanced responsibility of online platforms <https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms>

²⁸ Ibid.

²⁹ Internet Society Perspectives on Internet Content Blocking : An Overview (2017) <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/>

³⁰ Federal Communication Commission. Children’s Internet protection Act (CIPA) <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>

³¹ Kardefelt-Winther, D. (2017). How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? An evidence-focused literature review. Innocenti Discussion papers no. IDP_2017_12, UNICEF Office of Research – Innocenti, Florence. Available at: <https://www.unicef-irc.org/publications/925-how-does-the-time-children-spend-using-digital-technology-impact-their-mental-well.html>

³² LSE Media Policy Project Blog by Sonia Livingstone. New ‘Screen Time’ Rules from the American Academy of Pediatrics <http://blogs.lse.ac.uk/mediapolicyproject/2016/10/24/new-screen-time-rules-from-the-american-academy-of-pediatrics/>

³³ Lee, C., Kim, H., & Hong, A. (2017). Ex-post Evaluation of Illegalizing Juvenile Online Game after Midnight: A Case of Shutdown Policy in South Korea. *Telematics and Informatics*, DOI: 10.1016/j.tele.2017.07.006

³⁴ See, for example, Slavtcheva-Petkova, V., Jane Nash, V. & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. *Information, Communication & Society* Vol. 18, Iss. 1, 2015. Available at: <http://www.tandfonline.com/doi/full/10.1080/1369118X.2014.934387>

³⁵ Joe Cannataci, UN Special Rapporteur on Privacy <https://www.unicef-irc.org/article/1587-child-online-rights-and-privacy-in-focus-at-major-conference-in-brussels.html>

³⁶ This section draws on the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or GDPR) and The 7 Foundational Principles of Privacy by Design by Ann Cavoukian, former Information and Privacy Commissioner, Canada and Executive Director of Privacy and Big Data Institute, available at https://www.iab.org/wp-content/uploads/2011/03/fred_carter.pdf

³⁷ Privacy by design and privacy by default are two of the main principles of GDPR.

³⁸ For more information, see Deep Mind Ethics & Society <https://deepmind.com/applied/deepmind-ethics-society/> and DIPLO <https://www.diplomacy.edu/blog/artificial-intelligence-policy-implications>

³⁹ Global Commission on Internet Governance (2016). One Internet. CIGI and Chatham House. Available at: <https://www.cigionline.org/publications/one-internet>

⁴⁰ Council of Europe. Recommendation CM/REC (2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children’s rights in the digital environment (revised draft, 25 July 2017)

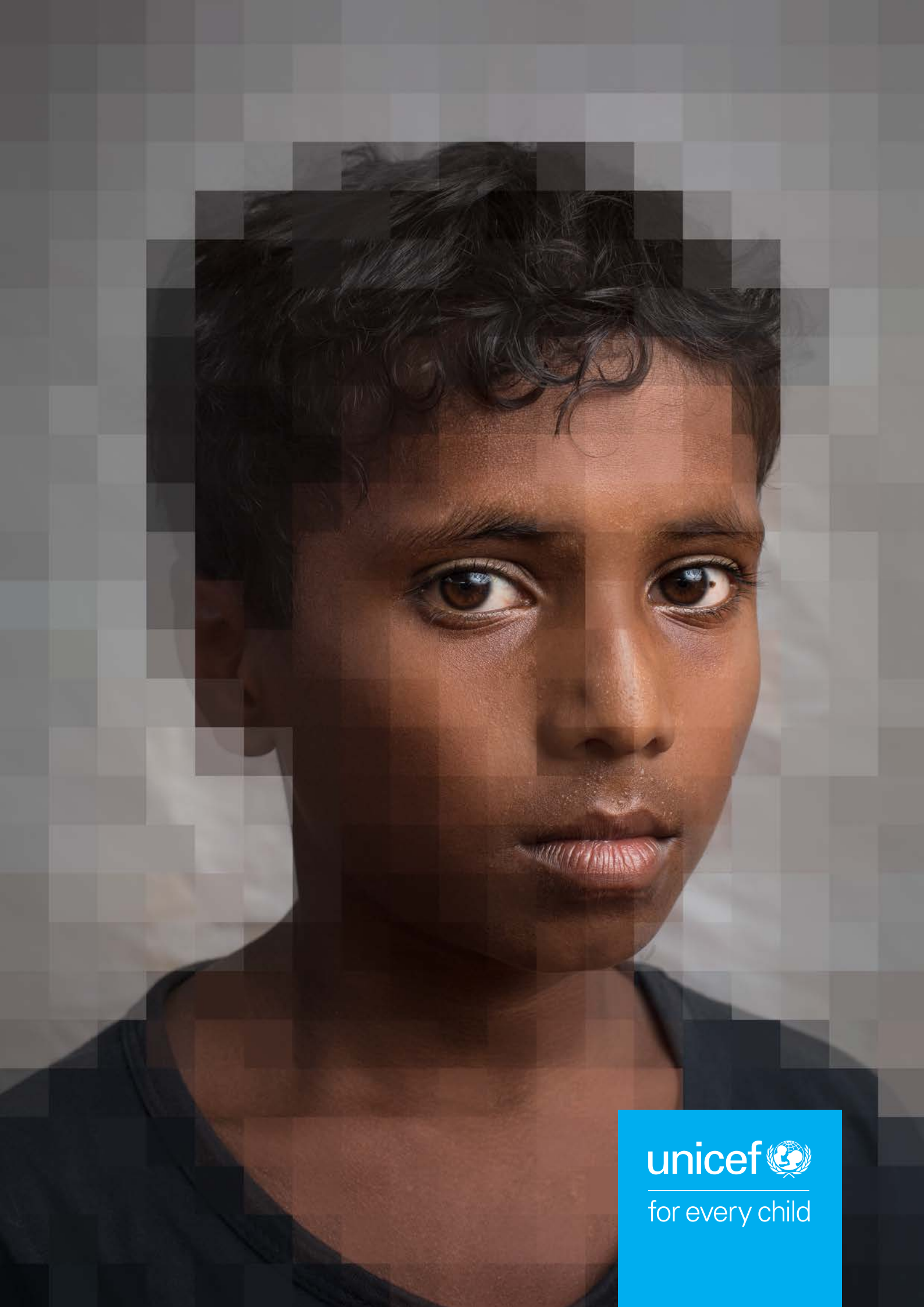
⁴¹ See, for example, World Economic Forum (2017) Digital Policy Playbook 2017: Approaches to National Digital Governance. White Paper. Available at: http://www3.weforum.org/docs/White_Paper_Digital_Policy_Playbook_Approaches_National_Digital_Governance_report_2017.pdf

⁴² Livingstone, Sonia, John Carr and Jasmina Byrne, One in Three: Internet Governance and Children’s Rights, discussion paper 2016-01, UNICEF Office of Research – Innocenti, 2016. Available at: <https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html>

⁴³ UNESCO. (2017). What if We All Governed the Internet? Advancing multistakeholder participation in Internet governance. Paris. Available at: <http://unesdoc.unesco.org/images/0025/002597/259717e.pdf>

⁴⁴ World Summit on the Information Society. Tunis Agenda for the Information Society. WSIS-05/TUNIS/DOC/6(Rev. 1)-E. 18 November 2005. <http://www.itu.int/net/wsisis/docs2/tunis/off/6rev1.html>

⁴⁵ Global Commission on Internet Governance (2015). Towards a Social Compact for Digital Privacy and Security. Centre for International Governance Innovation and Chatham House. Available at: https://www.intgovforum.org/cms/igf2016/uploads/proposal_background_paper/GCIG_Social_Compact.pdf



unicef 
for every child