5RIGHTS FOUNDATION

5Rights Foundation Contribution to the Global Digital Compact

April 2023

One in three users of digital services worldwide is a child, and the digital environment increasingly mediates all aspects of children's lives and has a growing impact on their development, physical and mental health, and well-being. The digital world has, however, not been developed with children in mind, and children's presence goes largely unrecognised and uncatered for by most of the digital platforms where children spend most of their time. As noted by Secretary-General Antonio Guterres in his "Our Common Agenda" report, the Internet is dominated by commercial interests and characterised by systematic digital surveillance and behavioural manipulation.[1] Children are particularly vulnerable to such exploitation. They are systematically exposed to a wide range of content, contact, conduct and contract risks.[2] Younger generations are increasingly suffering from egregious outcomes, including addiction, exposure to violent, radical and sexual content, hate speech, disinformation, cyberaggression and harassment, body dysmorphia, depression and self-harm, exploitation and abuse (including sexual), as well as economic exploitation.

The "open, free and secure digital future for all" envisaged by the Global Digital Compact requires the recognition of childhood online and the full implementation of the Rights of the Child in the digital environment. It is time to reset the Internet and build the digital world where children and young people can thrive.

As the joint position paper on behalf of the Child Rights Connect Taskforce points out: [3]

The digital environment plays an increasingly significant role across most aspects of children's lives. One in three internet users is a child, and, especially since the COVID-19 pandemic, children's development, relationships, education and play are increasingly mediated by digital technologies.

The digital environment is predominantly privately designed, owned, operated, and largely unregulated. Regulating and enforcing businesses' responsibility to respect children's rights, prevent and remedy abuse of their rights, including through providing children with a high level of privacy, safety and security by design and default, and upholding consistent global standards, is urgent for ensuring children's rights in the digital environment.

[1] Our Common Agenda, Report of the Secretary General, 2021, p. 62; https://www.riskyby.design/introduction.

[2] https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf , p. 62.

[3] Joint Submission to the Global Digital Compact "Key Priority Issues on Child Rights and the Digital Environment" on behalf of: Child Rights Connect, Alana Institute, ChildFund Alliance, Child Rights International Network (CRIN), ECPAT, Foundation for the Student Rights (Poland), Make Mothers Matter, Plan International, Plataforma de Infancia, Save the Children, SOS Children's Villages, Terre des Hommes International Federation, World Vision International and 5Rights Foundation.

Meaningful and equal access to safe digital technologies can support children to realise the full range of their civil, political, economic, social, and cultural rights. Children particularly value access to information and exchange, and to expression and having their voice heard. Yet millions of children have no access to the digital environment at all. There is a growing cost for children from the digital divide, including the gender-related digital divide.

Children are not a homogenous group; their agency, age and maturity, and different needs must be taken into account. Also, some children are disproportionately affected by the risks of the digital world, given the intersecting situations of vulnerability they may face. For instance, children with disabilities, girls, or children coming from different socioeconomic backgrounds face different barriers, including the digital divides. Thus, it is important to acknowledge that gender, age, disability, and other inter-sectional factors impact children's different experiences online, which must be carefully considered.

The digital environment must be safe for children and respect their full range of rights. At present, children's presence goes largely unrecognised and uncatered for on most of the digital platforms where children spend most of their time. Children are consequently exposed to a wide range of significant risks in the digital environment relating to content, contact, conduct and contract. These encompass, among other things, unfair terms, dark patterns, persuasive design, profiling and automated processes for user retention and information filtering. Children experience egregious outcomes, including addiction, exposure to violent, radical and sexual content, hate speech, disinformation, cyberaggression and harassment, body dysmorphia, gambling, exploitation and abuse, including sexual exploitation and abuse, as well as economic exploitation, including child labour and exploitation of their vulnerabilities for commercial purposes, and the promotion of or incitement to suicide or life-threatening activities. The growing impact on children's development, physical and mental health, and well-being is well-documented.

The obligations of States to respect, protect and fulfil child rights in the digital environment, as well as the responsibilities of the business sector to respect, prevent, mitigate and, where appropriate, remedy abuses are clearly explained in General comment No. 25.

States should prioritise two core actions:

1. Developing and implementing comprehensive policies and action plans for children's rights in the digital environment.[4]
2. Legislating to ensure business responsibility to respect children's rights, prevent and remedy abuse of their rights in relation to the digital environment.[5]

[4] See the Child Online Safety Toolkit: https://childonlinesafetytoolkit.org.

[5] Best practice legislation includes the UK's Age Appropriate Design Code: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/, the California Age-Appropriate Design Code: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273, and the EU's Digital Services Act: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

Overarching principles that should underpin all areas of the Global Digital Compact

Children have long-established rights and protections offline, and a life mediated by technology must be held to the same standards.

The 1989 United Nations Convention on the Rights of the Child (UNCRC) codified the rights of all under 18s, which are universal, inalienable, indivisible, interdependent, and interrelated. These rights apply in full in the digital environment, as set out in the 2021 UNCRC General Comment No. 25 (GC25).

The digital environment plays a central role in children's lives, and there are massive opportunities to harness it as a force for good for education, play, free expression and exchange. For this to be true, it must be designed with children's rights, interests and well-being front and centre. The Global Digital Compact (GDC) should, therefore, fully recognise and build on the UNCRC and its GC25 and be guided by the following principles:

1. **All under 18s have rights that must be protected and promoted**

A child is anyone under the age of 18 (Article 1, UNCRC), and all children, including teenagers, have the right to special considerations and the prioritisation of their best interests. Children are and must continue to be active and engaged participants of the digital world. We do not seek to protect children from the digital world but within it. Children should be heard and provided with protections and opportunities appropriate to their age and diverse needs.

2. **Children's rights apply wherever children are in practice, not only where we want them to be**

Children must be protected wherever they are online, not only on services specifically designed for them or targeting them. All services that children access or are likely to access must be safe for them and take their rights into account.

3. **Digital products and services must embed protections for children by design and default**

Privacy and safety measures for children must be built into each stage of product design and development processes. Organisations must think and act in anticipation of the risks to children rather than address harm after it occurs. They should build a high level of privacy, safety and security into the architecture and functioning of their services and apply these highest levels of protection by default for children.

The promotion, protection and implementation of children's rights in the digital environment must be a core principle of the UN Global Digital Compact and across all its thematic areas.

Protect data

In an increasingly connected world, everyday actions generate data - whether given by digital actors, observable from digital traces, or inferred[6]. Data drives many norms in the digital world. It creates opportunities for connection but can also be exploited or misused. While the digital environment was once seen as free and open, it has become increasingly privatised and controlled. Many seemingly free services require the currency of personal data in exchange for use. They are designed to gather and share consumers' data in ways that create profit for the business but can negatively impact the safety and well-being of children. The value and scope of this data collection often remain opaque to users, especially children.

Data protection is crucial for ensuring children's privacy, safety and security in the digital environment, which allows access to individuals and their data with unprecedented geographic reach and depth, along with much greater commercialisation of personal information.

There is a growing global consensus around the core principles for children's data protection,[7] which the Global Digital Compact should recognise, reflect and promote.

In a data-driven commercial environment, ensuring a high level of data protection for children is fundamental.

Actions to realise children's rights in the protect data theme:

States have a responsibility to ensure the developers and operators of digital services provide children with a high level of data protection by design and default and are held accountable.[8]

- States should take strong legislative and administrative measures to ensure any processing of children's data respects their rights and prioritises their best interests.[9]
- Such measures should integrate strong safety and privacy safeguards into the design of digital products and services accessing or processing the data of children[10]. They should also include transparency, independent oversight, access to remedy, and require accountability.[11]

---

[6] https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.
[7] See 5Rights Foundation, Approaches to Children's Data Protection: A Comparative International Mapping: https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf.
[8] UNCRC General comment No. 25; UNICEF Manifesto: https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf.
[9] Protecting children and their rights through child-centered data governance, prioritizing the best interests of the child in all decisions about their data, and taking into account children's unique identities, evolving capacities and circumstances are principles recognized by the Manifesto.: https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf.
[10] This is in line with the Report of the UN Special Rapporteur on the right to privacy: Artificial intelligence and privacy, and children's privacy which stresses that "the general elements of data protection by design, privacy by default, the right not to be subject to automated individual decision-making and data protection impact assessments are worthy of wider application for protecting the personal data of children".
[11] General comment No. 25 (2021), para 70.

- States should mandate service providers and operators undertake child data protection impact assessments and effectively mitigate any identified risks to children.
- States should prohibit practices that aim to manipulate children or influence their behaviour; that distort or impair children's ability to make autonomous and informed choices; that utilise children's data in ways that have been shown to be detrimental to their well-being; or that are designed to prioritise commercial interests over those of the child.[12]

Businesses have the responsibility to respect the rights of the child, take into account their best interests and implement the highest available industry standards of data protection for children by design and default.

- Businesses should undertake child rights due diligence, in particular by carrying out child data protection risk assessments covering content contact, conduct and contract risks to children and effectively mitigating any identified risks.
- Businesses should provide children with a high level of privacy, safety and security by design and default.
- Businesses should implement the highest available industry standards for children's data protection, age-appropriate design, age assurance, accessibility and transparency.
- Businesses must uphold their published terms, policies and community standards and provide effective mechanisms for children to exercise their data protection rights, reporting and redress.
- Businesses should provide prominent and accessible tools to help children exercise their data protection rights and report concerns.
- Businesses should involve children in the design and development of all digital products, services and features likely to be accessed by them.

[12] This echoes the mandates of data protection authorities meeting under the aegis of the Global Privacy Assembly in October 2021, which reiterates key elements of the UNCRC General Comment No. 25.

15 STANDARDS FOR CHILDREN'S DATA PROTECTION BY MEANS OF AGE-APPROPRIATE DESIGN

1. BEST INTERESTS OF THE CHILD

The best interests of the child should be a primary consideration when designing and developing digital services likely to be accessed by children. If there is a conflict between various interests (of users or stakeholders, including commercial interests), the service provider must prioritise the best interests of the child.

2. CHILD RIGHTS IMPACT ASSESSMENTS

Providers should undertake a Child Rights Impact Assessment to assess and mitigate risks to the rights and freedoms of children who are likely to access their service(s). They must consider differing ages, capacities, accessibility and development needs, and the full range of risks to children's privacy, safety and security, covering content, contact, conduct and contract risks.

3. AGE-APPROPRIATE APPLICATION

Providers must take a risk-based approach to recognise the age of individual users and ensure they effectively apply these standards to child users. They can either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children, or apply the standards to all their users. Any age assurance mechanisms in use must be privacy-preserving, proportionate, effective, age-appropriate, accessible, transparent and secure.

4. TRANSPARENCY

Published terms, policies and community standards, as well as privacy information, must be concise, prominent and in language and format that is clear and suited to the age of the child. Additional specific 'bite-sized' explanations should be provided at the point of use or feature activation.

5. DETRIMENTAL USE OF DATA

Children's personal data must not be used in ways that have been shown to be detrimental to their well-being or that go against industry codes of practice, other regulatory provisions or Government advice. This includes the use of personal data to extend engagement, recommend harmful content or actions, or unduly influence children's behaviour, notably via automated processes or dark patterns.

6. POLICIES AND COMMUNITY STANDARDS

Published terms, policies and community standards (including but not limited to privacy policies, age restrictions, behaviour rules and content policies) must be upheld, including by providing appropriate moderation and support in local languages.

7. DEFAULT SETTINGS

Default settings must respect children's rights Settings must be 'high privacy' by default (unless services can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child). Features designed to extend engagement or influence behaviour must be off by default.

8. DATAMINIMISATION

Only the minimum amount of personal data needed to provide the elements of a service in which a child is actively and knowingly engaged should be collected; child protection needs should not be construed as a reason to collect more data.

9. DATA SHARING

Providers and operators must not disclose children's data unless they can demonstrate a compelling reason to do so, taking into account the best interests of the child. Particular safeguards should be in place for data collected in educational settings.

10. GEOLOCATION

Geolocation settings must be off by default (unless there is a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Services must provide an obvious sign for children when location tracking is active Options which make a child's location visible to others must default back to 'off' at the end of each session.

11. PARENTAL CONTROLS

If parental controls are provided, children must be given age-appropriate information about this. If an online service allows a parent, carer or educator to monitor their child's online activity or track their location, an obvious sign must be given to the child when they are being monitored.

12. PROFILING

Options that use profiling must be switched 'off' by default (unless there is a compelling reason for profiling to be on by default, taking account of the best interests of the child). Profiling is only allowed if appropriate measures are in place to protect the child from any harmful effects (in particular, being fed content detrimental to their health or well-being. Profiling for targeted advertising is forbidden.

13. DARK PATTERNS

Practices that distort or impair children's ability to make autonomous and informed choices are prohibited. These include persuasive design strategies, gambling-style features, hidden costs, unfair terms and conditions, and techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.

14. CONNECTED TOYS AND DEVICES

Connected toys or devices must include effective tools to ensure a high level of privacy, safety and security for children.

15. ONLINE TOOLS

Prominent and accessible tools must be provided to help children exercise their data protection rights and report concerns.

Apply human rights online

Human rights apply online as they do offline, as do the rights of the child, which recognise and cater to children's specific vulnerabilities and development needs. How children's rights apply in the digital environment is set out in General Comment No. 25 to the UN Convention on the Rights of the Child. The Global Digital Compact must recognise and reiterate the core tenets of the UNCRC and General Comment No. 25 and highlight clear priorities for their effective implementation in the digital environment. It should also recognise and build on UNCRC General Comment No. 16 on state obligations regarding the impact of the business sector on children's rights.

Actions to realise children's rights in the Apply Human Rights Online theme:

The Global Digital Compact should drive the global commitment to the full implementation of children's existing rights in the digital world, as elaborated in UNCRC General Comment No. 25.

States have a responsibility to ensure their policy and legislative frameworks effectively implement children's rights in the digital environment.

- States should review and update their national policy frameworks to ensure a holistic and comprehensive approach to implementing children's rights in the digital environment.[13]
- States should take legislative and administrative measures to protect children in the digital environment. This should include regularly reviewing, updating, and enforcing robust legislative, regulatory and institutional frameworks that protect children from recognised and emerging risks of all forms of violence[14] in the digital environment. It should also take into account the voices of children and the diversity of their situations.
- States should legislate to enforce business responsibility to respect children´s rights and prevent and remedy abuse of their rights in the digital environment.[15]
- States should require businesses to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services.
- States should hold businesses accountable for infringements of children's rights facilitated by their products or services, including through the design and operation of digital services.

[13] In addition to the General comment No. 25, the 2021 OECD Recommendation on Children in the Digital Environment recognises the need to "Review, develop, and amend as appropriate, laws that directly or indirectly affect children in the digital environment".

[14] The Sustainable Development Goals 2030 ambitions a world that no longer tolerates violence against children. It thus requires that children must be protected online and offline.

[15] As set out in the UNCRC General comments No. 25 and No. 16.

- States should encourage businesses to actively engage with children, apply appropriate safeguards, and give their views due consideration when developing products and services.
- States should require businesses to provide children, parents, and caregivers with prompt and effective remedies and age-appropriate explanations of their terms of service.
- States should ensure access to justice for children's rights violations by providing for strong and effective monitoring, complaint, investigation, enforcement and redress mechanisms and ensuring systemic response. Complaint and reporting mechanisms should be free of charge, safe, confidential, responsive, child-friendly, and accessible.

Businesses have the responsibility to respect the rights of the child and implement the highest available industry standards to ensure their rights are taken into account by design and default.

- Businesses should undertake child rights due diligence, in particular by carrying out child rights impact assessments and effectively mitigating any identified risks.
- Businesses should provide children with a high level of privacy, safety and security by design and default.
- Businesses should implement the highest available industry standards for children's privacy and safety, age-appropriate design, age assurance, accessibility and transparency.
- Businesses must uphold their published terms, policies and community standards and provide effective mechanisms for children to exercise their rights, reporting and redress.
- Businesses should provide prominent and accessible tools to help children exercise their rights and report concerns.
- Businesses should involve children in the design and development of all digital products, services and features likely to be accessed by them.

As the joint position paper on behalf of the Child Rights Connect Taskforce points out: [16]

States parties must urgently review and update their national policy frameworks to ensure a holistic and comprehensive approach to implementing children's rights in the digital environment in line with the UNCRC. This should include the following:

- Identifying and building institutional capacity to ensure a holistic and coordinated approach to implementing children's rights in the digital environment across policies, programmes, government departments, industry sectors and geographies – taking into account children's views in all their diversity.
- Mobilising, allocating and utilising public resources to implement legislation, policies and programmes needed to address the increasing impact of the digital environment on children's rights and to promote the equality of access to, and affordability of, services and connectivity. Specific measures will be required to close the gender-related digital divide for girls. Children with disabilities and the development of assistive technologies should also be a special focus of attention.
- Undertaking a comprehensive review of national child protection policies and legislation to take full account of the digital environment and online-offline dynamics.
- Ensuring access to justice for children's rights violations in the digital environment by providing for strong and effective monitoring, complaint, investigation, enforcement and redress mechanisms, ensuring systemic responses to support and respond to crimes, including enabling effective investigation, reviewing sanctions and sentencing framework. Complaint and reporting mechanisms should be free of charge, safe, confidential, responsive, child-friendly, and available in accessible format. Particular attention should be paid to preventing and tackling gender-based violence and child sexual exploitation and abuse.
- Mandating child rights impact assessments (including child data protection impact assessments) to embed children's rights into legislation, budgetary allocations and other administrative decisions and procedures relating to the digital environment and promote their use among public bodies.
- Establishing a coordinated multi-stakeholder framework – including the technology sector and civil society organisations – to tackle risks and promote the exercise by children of their rights in the digital environment, including effective legal and regulatory enforcement mechanisms, prevention, remedies and access to expert advice on child online safety and well-being.

[16] Joint Submission to the Global Digital Compact "Key Priority Issues on Child Rights and the Digital Environment" on behalf of: Child Rights Connect, Alana Institute, ChildFund Alliance, Child Rights International Network (CRIN), ECPAT, Foundation for the Student Rights (Poland), Make Mothers Matter, Plan International, Plataforma de Infancia, Save the Children, SOS Children's Villages, Terre des Hommes International Federation, World Vision International and 5Rights Foundation.

- This should include promoting child-centred design, minimum standards, industry agreements, adoption of best practices and cultural awareness and resourcing of children's safety and well-being in the digital environment through regulation and enforcement of existing legislation and frameworks that relate to corporate responsibility.
- Identifying and filling knowledge and capacity gaps, including by strengthening and re-aligning the capacity and capability of law enforcement agencies and regulatory bodies in the child online safety field and providing training for professionals working for and with children, as well as the technology industry.
- Investing in awareness raising and education to prevent likely harms and promote positive internet use and the empowerment of children. This includes providing resources and support to teachers, parents and caregivers.
- Ensuring the respect and fulfilment of the right of the child to be heard in the digital environment, taking children's views and the diversity of their situations into account in the development of laws, policies and frameworks.
- Investing in and promoting research and data collection to inform legislation, policy and practice. States must improve their national data systems and ensure the measurement of the prevalence of child sexual exploitation and abuse to assess trends and progress towards its elimination.
- Recognising that the digital environment is an essential space to enable children to exercise their civil and political rights and facilitating the creation of empowering and safe digital spaces for child human rights defenders (CHRDs) and the exercise by children of their civil and political rights online. Ensuring that CHRDs, in all their diversity, can safely exercise their rights online free from harm and reprisals.

The business sector, including not-for-profit organisations, affects children's rights directly and indirectly in the provision of services and products relating to the digital environment. Businesses have the responsibility to respect children's rights, prevent and remedy abuse of their rights in relation to the digital environment, as set out in the UNCRC General comments No. 25 and No. 16. States parties have the obligation to ensure that businesses meet these responsibilities, and should develop, pass, and enforce legislation:

- Requiring businesses to undertake child rights due diligence, in particular, to carry out child rights impact assessments and effectively mitigate any risks posed by their products and services to children.
- Requiring businesses to recognise child users and take into account the diversity of their situations.
- Requiring the business sector to provide children with a high level of privacy, safety and security by design and default, enforcing the adoption of children's rights by design standards.
- Requiring businesses to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services, including for artificial intelligence.
- Holding businesses accountable for infringements of children's rights facilitated by their products or services, including through the design and operation of digital services.
- Prohibiting the unlawful digital surveillance of children by businesses, particularly in commercial settings and educational and care settings.
- Prohibiting the use of children's personal data and targeting of children using techniques designed to prioritise commercial interests over those of the child, including behavioural advertising.
- Requiring businesses to maintain high standards of transparency and accountability.
- Requiring businesses to provide children, parents, and caregivers with prompt and effective remedies.
- Requiring businesses to provide age-appropriate explanations to children, and to parents and caregivers for very young children, of their terms of service.
- Encouraging businesses to actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services.
- Encouraging businesses to take measures to innovate in the best interests of the child.
- Encouraging businesses to provide public information and accessible and timely advice to support children's safe and beneficial digital activities.

Regulation of artificial intelligence

AI-powered applications and devices increasingly mediate children's lives. From toys, video games and education tech to search, social media recommender systems and chatbots. AI is central to automated decision-making (ADM) systems and many other data-driven features common across digital services.

When AI systems directly interact with or impact children, there is a higher level of risk, given the specific vulnerabilities of children. Children cannot be expected to understand or take action against automated decision-making or algorithmic unfairness. It is unlikely that they have the developmental capacity, the knowledge or the resource to understand the subtle, cumulative or even acute nudges and impacts those automated systems have on their online experience. In fact, many children do not understand that an algorithm could be responsible for introducing them to a 'suggested friend', nor do they have the tools to prevent an onslaught of automated harmful material.

Considering AI-specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour[17]), AI systems which are not designed based on child-centred principles, trained on appropriate data sets and tested to ensure neutral or positive outcomes for children can have significant impacts on children's rights safety, privacy, cognitive development, health and educational outcomes, social relationships, economic well-being and freedoms[18].

To harness the enormous potential of AI as a positive force for education, play, freedom of expression, and exchange, it must be designed with the rights, interests, and well-being of children in mind.

Actions realise children's rights in the regulation of AI thematic:

Stakeholders should commit to ensuring the design, development and application of AI systems interacting or impacting children fully considers children's rights, needs and vulnerabilities.

In addition to the broader measures for all digital services, including AI systems set out above, with relation specifically to AI systems:

- States should introduce or update frameworks, legislation, regulations, and design standards that identify, define, and prohibit the use of AI systems that exploit children's vulnerabilities[19] as well as practices aimed at manipulating children or influencing their behaviour, that distort or impair children's ability to make autonomous and informed choices.
- Such measures should ensure requiring all providers and operators of AI systems likely to interact with or impact children undertake impact assessments and demonstrate that their systems do not manipulate or exploit child users, distort their

[17] https://www.vaia.be/files/cursusmateriaal/presentaties/VAIA-E-Lievens-Children-and-AI-240522.pdf.
[18] UNICEF's Initiative on AI and children's rights National AI strategies and children, Reviewing the landscape and identifying windows of opportunity, AI and Child Rights Policy Project, UNICEF, 2020.
[19] General Comment 25, para 62: States should ensure that automated systems or information filtering systems are not used to affect or influence children's behaviour or emotions or to limit their opportunities or development.

behaviour, or generate unfair or discriminatory outcomes for children. It must be clear that the burden of responsibility for the safety and respect of fundamental rights of child users rests primarily upon the AI providers and operators.

- The measures should also ensure that:
    - Children are not subjected to the same level of personal responsibility as adults for understanding risk.
    - Information and training for systems likely to be used by children are in a format and language that children can easily access and understand.
    - Sandboxing schemes for AI systems likely to interact with children or impact on children systematically use a diverse set of use cases and users and consider children's specific rights and needs.
    - Data collected in post-market monitoring include the age or age ranges of end users.
- States should introduce effective transparency and oversight mechanisms for all providers and operators of AI systems.[20]
- Businesses should uphold the highest available international standards for child-centred design and operation of AI systems.

[20] See 5Rights Foundation, Shedding Light on AI: A Framework for Algorithmic Oversight: https://5rightsfoundation.com/Shedding-light-on-AI---a-framework-for-algorithmic-oversight.pdf.

A global, consistent, and enforceable standard

While the digital divide is commonly measured by differences within and between countries in areas such as digital literacy, access to bandwidth, use of sophisticated devices, platforms, and educational resources, the lack of legislation specifically addressing children's safety online, privacy and data protection is another facet of the digital divide.

Since only a handful of countries have adopted rules and legislation or established adequate institutional arrangements, the safety, security and privacy flaws offered to young people vary according to their geographical location, despite their use of a "global product".

This gap in child online safety, data protection, privacy, ownership, governance, and security - with specific reference to children – is part of the broader digital divide and requires a global approach and commitment.

The challenges the technology sector poses are transnational and therefore require a global approach and commitment. The Global Digital Compact priority should be underpinned by a desire to see global, consistent, and enforceable standards that can be implemented across jurisdictions.

To ease compliance and close any regulatory loopholes, a patchwork of internationally inconsistent regulation must be avoided. The Global Digital Compact should commit to using the following existing frameworks and tools that reflect best practices and providing strong and unambiguous requirements for the protection of children and a benchmark against which any initiatives should be judged so coherent action can deliver for children – wherever they are:

- The UK Age Appropriate Design Code represents a global standard for protecting children's rights and privacy online. It transforms how companies collect, share and use children's data by requiring them to offer children a high level of privacy protection by default. The ground-breaking Code has ushered in a paradigm shift, as it applies to all child users under 18. It focuses on all services children are likely to access, or where it is reasonably foreseeable, they will access, not merely those designed for and targeted at them. The Code has shown that the digital world can not only be changed but improved – and that the boundless creativity of the tech sector can be placed at the service of children and their best interests rather than forever more 'engagement '. Global tech companies have already demonstrated their ability to deliver age-appropriate designs under the UK and statutory requirements in Ireland. Companies are also readying to meet such requirements in California, where they go into effect in July 2024. Those benefits should be rolled out worldwide to consolidate a global standard to drive responsible innovation and a better internet for all.
- The Child Online Safety Toolkit is an actionable, practical Step-by-step roadmap for policymakers to develop policies for online child safety. It provides functional guidance to turn principles into action and enshrine child online safety into law and practice. It was designed to be universally applicable in every context, building upon the ITU Guidelines on Child Online Protection, General Comment No. 25, WeProtect's Model National Response (MNR) and the UN's Secretary General's Roadmap for Digital Cooperation.

- The IEEE 2089-2021 Standard for Age-Appropriate Digital Service Framework introduces practical steps that companies can follow to design age-appropriate digital products and services to design digital services with children in mind. It is informed by children's existing rights under the UNCRC.
- The Digital Futures Commission toolkit Child Rights by Design sets out principle-based design considerations to help digital innovators embed children's rights into digital products and services, taking the lead from the UN Committee on the Rights of the Child's authoritative statement, General Comment No. 25.

About 5Rights Foundation

5Rights develops new policies, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities.

Our focus is on implementable change, and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children so that digital products and services can impact positively on the lived experiences of young people.