

Strasbourg, 25 July 2017

CAHENF-IT(2017)9

**Ad hoc Committee for the Rights of the Child (CAHENF)**

**Drafting Group of Specialists on Children and the Digital Environment (CAHENF-IT)**

**Working title: 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)**

|  |
| --- |
| In accordance with its terms of reference, and in line with the Council of Europe Strategy for the Rights of the Child (2016-2021), the Ad Hoc Committee for the Rights of the Child (CAHENF) is elaborating guidelines for member states to promote, protect and fulfil children’s rights in the digital environment, with the support of its drafting group (CAHENF-IT). The elaboration of the draft instrument started in 2016 and is expected to be completed by November 2017.  A wide consultation of key actors and civil society has been scheduled before finalising the preparation of the future legal instrument, in order for the Committee to be able to consider their point of views and experiences.  A written consultation on the instrument is now open. Comments on the draft instrument should be sent to the CAHENF Secretariat ([children@coe.int](mailto:children@coe.int)) in English or French, by **4 September2017**at the latest. |

**Working title: 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)**

*Preamble*

The Committee of Ministers, under the terms of Article 15*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve greater unity between its members for the purpose of safeguarding and promoting the ideals and principles which are their common heritage, inter alia by promoting common policies and standards,

Bearing in mind the Council of Europe Strategy for the Rights of the Child (2016-2021) which identified the rights of the child in the digital environment as one of its priority areas and the Council of Europe Strategy on Internet Governance (2016-2019) according to which the internet should be a safe, secure, open and enabling environment for everyone, children included, without discrimination,

Reaffirming the commitment of member states to ensure that children enjoy the full range of human rights enshrined in the United Nations Convention on the Rights of the Child (UNCRC), in the European Convention on Human Rights (ETS No. 5), and their protocols, and that these rights should continue to be protected regardless of new technological developments,

Taking into account all relevant international and European conventions and legal instruments, notably the European Convention on the Exercise of Children’s Rights (ETS No. 160), the revised European Social Charter (ETS No. 163), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), the Convention on Cybercrime (ETS No. 185), the Convention on Action against Trafficking in Human Beings (CETS No. 197), the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201),

Recalling the following recommendations of the Committee of Ministers to member states: CM/Rec(2016)5 on Internet freedom, CM/Rec(2016)2 on the Internet of citizens, CM/Rec(2016)3 on human rights and business, CM/Rec(2015)6 on the free, transboundary flow of information on the Internet, CM/Rec(2014)6 on a Guide to human rights for Internet users, CM/Rec(2013)1 on gender equality and media, CM/Rec(2012)6 on the protection and promotion of the rights of women and girls with disabilities, CM/Rec(2012)4 on the protection of human rights with regard to social networking services, CM(2012) on the protection of human rights with regard to search engines, CM/Rec(2012)2 on the participation of children and young people under the age of 18, CM/rec (2011)7 on a new notion of media, CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, CM/Rec(2010)8 on youth information, CM/Rec(2009)10 on integrated national strategies for the protection of children from violence, CM/Rec(2009)1 on electronic democracy, CM/Rec(2009)5 on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, CM/Rec(2007)3 on the remit of public service media in the information society, CM/Rec(2007)16 on measure to promote the public service value of the internet, Rec(2006)12 on empowering children in the new information and communication environment, Rec(2001)8 on self-regulation concerning cyber content (self-regulation and user protection against illegal and harmful content on new communications and information services);

Having regard to the following declarations of the Committee of Ministers to member states: the Declaration on protecting the dignity, security and privacy of children on the Internet (2008), Declaration on freedom of communications on the Internet (2003);

Bearing in mind the following recommendations and resolutions of the Parliamentary Assembly of the Council of Europe: Resolution 2144 (2017) on “Ending cyberdiscrimination and online hate”, Resolution 2103 (2016) on “Preventing the radicalisation of children and young people by fighting the root causes”, Recommendation 1980 (2011) on “Combating ‘child abuse images’ through committed, transversal and internationally coordinated action”, Recommendation 1836 (2008) on “realizing the full potential of e-learning for education and training”, Recommendation 1882 (2009) on the “The promotion of internet and online media services appropriate for minors”, Recommendation 1466 (2000) on “Media education”;

Recalling the recommendations of the United Nations Committee on the Rights of the Child that all children should be able to safely access ICTs and digital media, and be empowered to fully participate, express themselves, seek information and enjoy all the rights enshrined in the UNCRC and its Optional Protocols without discrimination of any kind;

Recognising that the digital environment is complex and subject to rapid evolution, and is reshaping children’s lives in many ways, resulting in new opportunities for and risks to their well-being and rights;

Conscious that information and communication technologies are an important tool in children’s lives for learning, socialisation, expression, inclusion and fulfilment of the rights of the child and fundamental freedoms, for their protection from violence, exploitation and abuse; while at the same time, they can generate risks of evolving forms of violence and facilitate the commission of criminal activities against children;

Determined to contribute effectively to ensuring that consistent policies are being developed that take into account the interdependence of opportunities and risks in the digital environment and the need to ensure that appropriate measures are in place so that children’s rights are protected, promoted and fulfilled;

Emphasising that States have the primary responsibility to respect, protect and fulfil the rights of the child and reaffirming the responsibilities, rights and duties of the parent(s), legal guardian(s) or other any other person who has the care of the child to provide, in a manner consistent with their best interests and evolving capacities of the child, appropriate direction and guidance in the exercise by the child or his or her rights;

Recognising also that the private sector has a responsibility to respect human rights, including children’s rights, as confirmed in CM/Rec(2016)3 on human rights and business, the UN Committee on the Rights of the Child’s General Comment No. 16 on State obligations regarding the impact of the business sector on children’s rights, the UN Guiding Principles on Business and Human Rights, the Council of Europe guidelines for law enforcement and service providers (2008), the Human Rights Guidelines for Internet Service Providers and for Online Games designers and publishers (2008), and the Children’s Rights and Business Principles developed by UNICEF, the UN Global Compact and Save the Children;

Conscious that policies in this area require a combination of public and private, legal and voluntary measures at various levels, and that all relevant public and private actors share responsibility for ensuring children’s rights in the digital environment, and coordination of their actions is necessary;

Recognising the need to develop guidance to assist states and other relevant actors in their efforts to develop comprehensive strategies to promote, protect and fulfilchildren’s rights in the digital environment, rooted in the United Nations Convention on the Rights of the Child and Council of Europe standards, which are developed with children’s participation;

Recommends that governments of Member States:

1. review their national legislation, policies and practice, to ensure that they integrate the recommendations and guidance set out in Appendix I of this recommendation, and evaluate the effectiveness of the measures taken at regular intervals;
2. ensure the widest possible dissemination of this Recommendation among competent authorities and stakeholders and promote the implementation of these guidelines in all relevant areas, including any which, while not impinging directly on the competencies of public authorities, are nonetheless important in the context of children’s rights;
3. encourage the private sector to engage in genuine dialogue with relevant state actors, civil society and children and to take implementing measures, taking into account the UN Guiding Principles on Business and Human Rights, the Council of Europe Recommendation (2016)3 on human rights and business, and the Children’s Rights and Business Principles developed by UNICEF, the UN Global Compact and Save the Children;
4. co-operate with the Council of Europe by developing, implementing and monitoring strategies and programmes that promote, protect and fulfil children’s rights in the digital environment, and share, on a regular basis, examples of strategies, action plans and good practices related to the implementation of this Recommendation*;*
5. *examine within the Committee of Ministers progress in the implementation of this Recommendation no later than five years after its adoption, with the participation of relevant stakeholders.*
6. **Appendix to the Recommendation**
7. **Purpose and aims**

The present Guidelines are intended to enhance the implementation of the rights and existing principles enshrined in the instruments referred to in the preamble and the case law of the European Court of Human Rights. They seek in particular to:

1. guide States to integrate into their legislation and implement the policies, practices, principles and actions set out in these guidelines, in order to promote the realisation of the full array of children’s rights in the digital environment and address the full range of ways in which the digital environment impacts on children’s rights and well-being;
2. promote the development, implementation and monitoring by States of an integrated approach, reflecting the principles contained in the present Guidelines;
3. ensure that States, as appropriate, require, encourage and support business enterprises and other relevant actors to meet their responsibilities to promote and respect children’s rights in the digital environment;
4. strengthen national and international co-operation to fulfil children’s rights in the digital environment.
5. **Definitions and terminology used for the purpose of the Guidelines**
6. **“Child”** shall mean any person under the age of 18 year.
7. **“Digital environment”** shall mean information and communication technologies, including the internet, its associated technologies and digital media. Information and communication technologies refers to all technical means used to handle information and aid communication, including both computer and network hardware as well as necessary software such as mobile phones, tablets, digital cameras and any other smart devices.
8. **“Hashes”**: images of child sexual abuse converted into and stored as encrypted files, which constitute a unique digital finger print Hashes can be deployed to analyse rapidly vast amounts of data without the necessity for law enforcement officers or others having to look at every image found on a suspect’s device.
9. **“Personal data”:** any information relating to an identified or identifiable child (data subject).
10. “**Processing”:** any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.
11. **“Self-generated sexual content”:** refers to images and videos depicting sexually explicit conduct or any depiction of a child’s sexual organs or other types of sexual images and/or videos made or apparently made by the children themselves on their own initiative.
12. **“Sensitive data”:** special categories of data covered by Convention ETS 108, which require complementary appropriate safeguards when they are processed.
13. **Fundamental principles and rights**
    1. *Best interests of the child*
14. In all actions affecting children’s rights in the digital environment, the best interests of the child should be the primary consideration.[[1]](#footnote-1) Every child, as an individual rights-holder, should be able to exercise his or her human rights and fundamental freedoms online as well as offline.[[2]](#footnote-2) States should promote the realisation of the full array of children’s rights in the digital environment, including the right to life and the right to survival and development[[3]](#footnote-3). This includes the obligation to address the ways in which society’s use of digital media has consequences for children’s rights and well-being.
15. In assessing the best interests of a child, states should make every effort to balance and wherever possible reconcile a child’s right to protection with other rights, in particular the right to freedom of expression and child participation rights.
    1. *Right to non-discrimination*
16. The rights of the child apply to all children regardless of their or their parents’ sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth, sexual orientation or gender identity, state of health, disability or other status.[[4]](#footnote-4)
17. Whereas efforts should be undertaken to promote, respect and fulfil the rights of each and every child in the digital environment, targeted measures may be needed for children in vulnerable situations, recognising that the digital environment has the potential both to increase their vulnerability and also to empower and support them.
    1. *Right to be heard*
18. Children have the right to express themselves freely on all matters affecting their lives, and their views should be given due weight in accordance with their age and maturity.[[5]](#footnote-5) States and other relevant actors should provide children with information appropriate to their maturity and circumstances on their rights, including their participation rights, and enhance opportunities for them to express themselves freely through the media and information and communication technologies as a complementary tool to face-to-face participation. Children should be informed about mechanisms providing adequate support, procedures for complaints, remedies or redress.
19. Furthermore, relevant actors should actively engage children, taking into account their evolving capacity, to participate meaningfully in the development, implementation and evaluation of policies, mechanisms, practices, technologies and resources that aim to promote, protect and fulfil their rights in the digital environment.
    1. *Evolving capacities of children*
20. Although all children from birth to the age of 18 have the same rights, their capacities develop gradually during that timeframe[[6]](#footnote-6). Moreover, individual children may reach different levels of maturity at different ages.[[7]](#footnote-7) States and other relevant actors should recognize the evolving capacities of children, including those of children with disabilities, and ensure that policies and practices are adopted to respond to their respective needs in relation to the digital environment. This also means, for example, that policies adopted to ensure the realisation of the rights of adolescents may differ significantly from those adopted for younger children.[[8]](#footnote-8)
    1. *Stakeholders’ obligations and responsibilities*
21. In accordance with relevant international standards, the State has the primary obligation to respect, protect and fulfil the rights of all children within its jurisdiction and must engage all relevant stakeholders, including public and business enterprises, civil society, as well as children themselves and their parents and carers, in order to ensure the effective implementation of these obligations.[[9]](#footnote-9)
22. In the context of the digital environment, states should apply such measures, as may be necessary, to require that business enterprises operating within their territorial jurisdiction, and as appropriate, throughout their operation abroad when domiciled in their jurisdiction, respect children’s rights. They should adopt effective enforcement measures with respect to business standards and children’s rights in the digital environment, and ensure that relevant regulatory bodies are effectively engaged.
23. **Operational principles and measures to empower, protect and support children’s rights in the digital environment** 
    1. *Access to and use of the digital environment*
24. Access to and use of the digital environment is important for the realisation of children’s rights and freedoms, as well as their inclusion, participation and for maintaining family relationships[[10]](#footnote-10). Limited or no access to the digital environment can deprive children of the ability to exercise fully their human rights.
25. States should make appropriate arrangements to ensure adequate access to devices, connectivity, services and content for all children, with a view to ensuring that this provision is available, affordable and secure for all children.
26. States should ensure that access to the digital environment is provided in educational and other care settings for children. Specific measures should be taken for children in vulnerable situations, in particular children living in foster homes, children deprived of liberty or whose parents are deprived of liberty, migrant children, and children in rural communities.
27. Access to devices, connectivity, services and content should be available in the child’s language and accompanied by appropriate education and literacy measures, including those which address gender stereotypes or social norms that could limit children’s access and use of technology. In particular, States should require online service providers to ensure their services are accessible by children with disabilities.[[11]](#footnote-11)
28. States should ensure that terms and conditions that are associated with the use of a device which can connect to the Internet or that apply to the provision of any online service are accessible, fair, transparent, intelligible, and formulated in clear and plain language, including in child-friendly language, where appropriate.
29. States should ensure plurality of sources of high quality information and educational content for children. The child’s best interests should be taken into account in related public procurement procedures so that digital services and contents used by children are not unduly restricted by commercial interests or safety filters.
    1. *Right to freedom of expression and information*
30. The digital environment has considerable potential to support the realisation of children’s right to freedom of expression, including to seek, receive and impart information and ideas of all kinds.[[12]](#footnote-12)
31. States should take measures to guarantee children’s right to hold and express any views, opinions or expressions on matters of importance to them and through the media of their choice, irrespective of whether or not they are received favourably by the State or others.[[13]](#footnote-13)
32. As creators and distributors of information, children should be made aware that the exercise of their right to freedom of expression carries duties and responsibilities, for instance, to respect the rights of others.
33. States should initiate and encourage the provision of high quality online content and services of social and cultural benefit for children in support of their fullest development and participation in society. This should include the greatest possible provision of high quality content that is specifically made for them, easy for them to find and understand, and provided in their language.[[14]](#footnote-14) Particularly important is information about rights and responsibilities, as well as about news, health, sexuality and identity, among other resources of benefit to them.
34. Any restrictions on children’s right to freedom of expression and information in the digital environment should comply with international human rights standards on freedom of expression.[[15]](#footnote-15) States should take measures to ensure children are informed of any restrictions on this right, such as content filtering, in a manner appropriate to their evolving capacities and including guidance on how and to whom to make a complaint, report an abuse or request help and counselling. Parents and caregivers should also be informed of such restrictions and appropriate remedies.
    1. *Participation, right to play, and right to assembly and association*
35. The digital environment provides distinctive opportunities for children’s rights to freedom of peaceful assembly, association, and play through online communication, entertainment and participation, including creating and maintaining social relationships, play, and sharing experiences and activities with others. States should co-operate with other stakeholders to promote such activities for children, recognising that online engagement can foster participation, inclusion, citizenship and resilience both online and also offline.
36. States should provide a range of incentives, investment opportunities, standards and technical guidance for the production and distribution of digital content and services of social, civic and cultural benefit for all children, including interactive and play-based tools appropriate to their evolving capacities and with particular attention to the needs of children in vulnerable situations. Where children participate in their production, measures in place should protect the intellectual property of young creators.
37. States should provide children and young people with information appropriate to their age and circumstances, including in non-written forms and through social networking and other media, on their rights, and in particular their participation rights, the opportunities available to them to do so and where they can get support to take advantage of these opportunities.
38. States should adapt their legal frameworks to ensure that children are able to engage effectively in local, national and global public policy and political debates and participate in online civic and social platforms, strengthening their capacity for democratic citizenship and political awareness. They should also ensure that children’s participation in the digital environment is heard and acted upon meaningfully, building on existing good practice for child participation and available tools for assessment.
39. States should take steps to ensure that monitoring and surveillance of assembly and association of children in the digital environment should not take place and that any exceptions to this must comply with those provided for in Article 11 paragraph 2 of the ECHR.
40. Where States make provision for public service media, these should involve children in active forms of communication, encouraging the provision of user-generated content and establishing other participatory schemes. Attention should also be paid to children’s access to, and presence and portrayal in, public service media online.
    1. *Privacy and data protection*
41. Children must not be subjected to arbitrary or unlawful interference with their privacy in the digital environment.[[16]](#footnote-16) Any restriction on the child’s right to respect for privacy should comply with international human rights standards. Developing effective safeguards against arbitrary or unlawful interference with a child’s right to privacy should also not unduly restrict other rights, such as freedom of expression or participation.
42. States must undertake every effort to protect children’s privacy, personal data, online reputation and to respect the confidentiality of their correspondence, and ensure that relevant actors, including the child’s peers, parents or caregivers, business enterprises, do the same[[17]](#footnote-17).
43. States should take measures to ensure that children’s personal data is processed fairly and lawfully, accurately and securely, with the unambiguous, free, specific and informed consent of the child and/or their legal representative, or in accordance with another legitimate basis prescribed by law.
44. States should take measures to limit to the greatest extent possible the processing of children’s personal data by any actor. In particular, the collection or use of sensitive data, for example concerning racial or ethnic origins, political opinions, religious or other beliefs, mental and physical health, sexual life, or genetic or biometric data, should in all instances be provided for by law and comply with the strictest safeguards.[[18]](#footnote-18)
45. States should ensure that the likely impact of an intended data processing on children’s rights is assessed and the data processing should be designed in such a manner to prevent or minimize the risk of interference with those rights.
46. States should implement, and where appropriate require relevant stakeholders to implement, privacy-by-default settings and privacy-by-design measures, taking into account the best interests of the child. Such measures should integrate high safeguards for the right to privacy into devices and services.
47. States should ensure that easily accessible, meaningful, child-friendly and age-appropriate information about privacy tools and settings is made available to children. Children and their parents or legal representatives should be informed how their personal data is being processed, for instance how it is collected, stored, used and shared with others when it is the case, and what rights they may have to require access to their data or require that such data is corrected or erased, as well as how to exercise these rights.
48. States should ensure that children have the right to have their personal data erased when they withdraw their consent or object to the processing of personal data concerning them, especially where this compromises their dignity, security and privacy.
49. Where States take measures to decide upon an age at which a child would be considered to be capable of consenting to the processing of personal data, children’s rights and views, the best interests and the evolving capacities of children must be taken into consideration. The adequacy of age thresholds must be monitored and evaluated in light of children’s actual understanding of data collection practices and technological developments.
50. In the context of the emergence of connected or smart devices, including those incorporated in toys and clothes, States should ensure that data protection principles and rights are respected when such products are directed principally at children or are likely to be regularly used in physical proximity to children.
51. Profiling of children, which is an automatic data processing technique which produces an online “profile” of a child, particularly in order to take decisions concerning him or her or for analyzing or predicting her or his personal preferences, behaviors and attitudes, should be prohibited by law. In exceptional circumstances, States may lift this restriction when this is in the legitimate interest of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law.[[19]](#footnote-19)
52. Surveillance or interception measures which may affect children’s rights must be carried out in accordance with the law, pursue a legitimate aim, be necessary in a democratic society and be proportionate to the legitimate aim pursued. They should be subject to effective, independent and impartial oversight. Where appropriate, children should be informed that such data in respect of them has been collected and what rights they may have to require such data to be corrected or erased, as well as how to exercise these rights.
53. States should not prohibit anonymity, pseudonymity or the usage of encryption technologies, by law or in practice, for children. Any restrictions should be subject to the requirements of legality, legitimacy and proportionality, in line with international human rights standards.[[20]](#footnote-20)
    1. *Education and digital literacy*

1. States should actively invest in and promote the opportunities offered by the digital environment to realize the child’s right to education. The goal of education is the development of the child's personality, talents and mental and physical abilities to their fullest potential, and the preparation of the child for responsible life in a free society. In support of this goal, it is important that the knowledge and resources of the digital environment are available to all children in a way that is inclusive and takes into account children’s evolving capacities and the particular circumstances of children in vulnerable situations.

*Digital literacy*

1. Digital States should promote the development of digital literacy, including media and information literacies, as part of the basic education curriculum and from the earliest years, in accordance with children’s evolving capacities. In support of a wide range of children’s rights, digital literacy and education should include the technical or functional competences to use a wide range of online tools and resources, and also content creation and critical understanding of the digital environment. It should also include knowledge of their rights and the rights of others, as well as of responsibilities, in relation to the digital environment.
2. Particular efforts should be made by States and other relevant actors through the educational and cultural system to support and promote the digital literacy of: a) children who have no or little access to digital technology for socio- geographical or socio-economic reasons, as well as sometimes for reasons of place of residence; b) children who have access to but do not use, lack the skills to use or underuse digital technology for reasons of vulnerability or circumstance.
3. Literacy should be effectively promoted through the settings where children and parents or caregivers use the internet, especially schools, and through the State’s established mechanisms for reaching parents.
4. Formal and non- formal educational and cultural institutions (including libraries, museums, youth centres and other learning institutions) should be supported and encouraged to develop and make available a plurality of digital and interactive learning resources and to cooperate across institutional boundaries to optimise learning opportunities in relation to the digital environment.

*Educational programmes and resources*

1. States should ensure that sufficient high quality educational resources are available in the digital environment. These may be developed and distributed in co-operation with other relevant actors, and should support children’s formal and also non-formal and informal education. Such provision should be evaluated according to current good practice and necessary actions taken by States and others to maintain high standards of education relevant to the digital environment.
2. States should ensure the development and availability of awareness-raising efforts, user tools and education programmes for children and parents or caregivers to enable benefits and prevent and respond to risks in the digital environment, with the involvement of children. This should include support for skills that enable children to better understand and deal with potentially harmful content (such as violence and self-harm, pornography, discrimination and racism) and behaviour (such as grooming, bullying or harassment), thereby promoting confidence, well-being and respect for others in the digital environment. To address child exploitation online, states should implement, within nationwide education programmes, specific child exploitation primary prevention education programmes.

*Investment and training*

1. States should ensure investment in digital hardware, software, connectivity and training in schools to support learning.
2. States should ensure that initial and in-service training informs and empowers educators so they can support children in acquiring the skills and literacies needed to exercise their rights related to the digital environment.
   1. *The right to protection and safety*
3. Children must be afforded protection from the risk of harm to their physical and mental welfare, in particular regarding sexual exploitation and abuse. As regards harmful content and behaviour online, children are entitled to special care and assistance that is appropriate to their age and circumstances. This is particularly relevant with regard to the risk of harm which may arise from online pornography, the degrading and stereotyped portrayal of women, the portrayal and glorification of violence and self-harm, in particular suicides, demeaning, discriminatory or racist expressions or apologia for such conduct, solicitation for sexual abuse purposes, the online recruitment of children for committing criminal offences or for trafficking; bullying, stalking, and other forms of harassment, all which are capable of adversely affecting the physical, emotional and psychological well-being of a child. Measures taken to protect children in the digital environment should take into consideration the best interests and evolving capacity of children and not restrict unduly the exercise of their other rights.

*Online protection and safety policy and awareness-raising*

1. Existing standards and guidance, such as the Council of Europe policy guidelines on integrated national strategies for the protection of children from violence, should be taken into consideration when developing a comprehensive online protection and safety policy framework.
2. States should develop and strengthen education and awareness-raising programmes for children, parents or caregivers, and educators on the right to respect for human dignity, respect for privacy and safety in the digital environment, the impact of self-generated content, as well as potential consequences of the way in which information about children might be shared in different settings and by others, how to prevent, identify, report violations of their rights and seek redress.
3. States should encourage businesses enterprises and any other relevant actors to help promote awareness of the online protection and safety policy framework, in particular to children, parents, teachers and the general public.

*Specific measures by business enterprises*

1. States should take measures to promote safety-by-design as a guiding principle for devices produced for or services addressed to or used by children, including addressing the risk of excessive use and sleep deprivation.
2. States should require the use of effective age-verification systems to ensure children are protected from products and services which are legally restricted by reference to specific ages, for example the sale of alcohol, tobacco, weapons and gambling or exposure to content which in the physical world would ordinarily be subject to age restrictions, for example pornography.
3. States should require business enterprises to take reasonable, proportionate and effective measures to ensure that their networks or online services are not misused for criminal or other unlawful purposes in ways which may harm children, such as for example with regard to the distribution or storage of child sexual abuse material.

*Specific requirements for the Registry for a country code top level domain*

1. States should include clear requirements when awarding a contract or license to an entity to become the Registry for a country code top level domain to have due regard to the best interests of children. Such requirements should cover, for example a clear prohibition by the Registry of the registration or use of any domain name which advertises or suggests that child sexual abuse material may be available and the establishment by the Registry of mechanisms to ensure this policy is enforced, including by Registrars and Registrants.
2. Where a Registrant proposes to establish a child oriented site or service within their country code domain, States should ensure that the Registry requires Registrants to put in place appropriate child protection policies.

*Measures to address cyber-bullying and cyber-grooming*

1. States should share good practices on ways to prevent cyber-bullying and cyber-grooming. In this connection, age-differentiated access should be treated carefully where age is provided by children and young people themselves.
2. In situations of victimization of a child, for example by a peer or cyber-bullying cases, the State should as far as possible pursue suitable and adequate preventative and restorative approaches that repair the harm done, while preventing the criminalisation of children.[[21]](#footnote-21)
3. States should require social networking providers to take diligent action in response to complaints of cyber- bullying and cyber-grooming.

*Policies and measures regarding illegal or harmful content and material, including child abuse material*

1. States should ensure there is an effective mechanism to allow any person to report suspected illegal or harmful material found online, in particular material which depicts child sexual abuse, such as for example hotlines.
2. Policing with respect to child abuse material should be victim-focused with the highest priority being attached to identifying and locating child victims depicted in images, and ensuring wherever possible that any harmful elements in their environment are addressed. In particular, States should take steps to ensure that local law enforcement agencies establish databases of “hashes” and expedite actions to locate victims or identify and take action against offenders.
3. States should monitor trends in terms of hosting child abuse material within their jurisdiction, and, mindful of available technologies, ensure that all necessary steps are being taken by business enterprises to delete promptly any images found on local servers and, pending its deletion, restrict access to illegal images found on servers.
4. Recognising that the hashes cannot be reverse engineered to create child abuse images, States should encourage relevant business enterprises to construct and maintain hash lists in order to help them ensure their networks are not being misused to store or distribute child abuse images.
   1. *Remedies*
5. Member States should ensure the effective implementation of their obligations under Articles 6 and 13 of the European Convention on Human Rights and other international and European human rights instruments, to ensure a child’s right to an effective remedy when their human rights and fundamental freedoms have been abused or violated in the digital environment. This entails the provision of available, known, accessible, affordable, and child-friendly avenues through which children, as well as their parent(s) or legal representative(s), may submit complaints and seek remedies. Effective remedies can include, depending on the violation in question, inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation[[22]](#footnote-22).
6. States should ensure that in all cases, access to courts or judicial review of administrative remedies and other procedures is available, in line with the principles set out in the Council of Europe Guidelines on Child-Friendly Justice.
7. In addition to judicial remedies, States should ensure the availability of appropriate State-based non-judicial mechanisms, such as national human rights institutions, child ombudsperson institutions[[23]](#footnote-23). The availability, adequacy and effectiveness of these mechanisms for handling cases of violations or abuses of children’s rights in the digital environment should be reviewed on a regular basis.
8. States should also encourage business enterprises to establish their own remedial and grievance mechanisms, in line with the effectiveness criteria of the UN Guiding Principles, while ensuring that they are not used to impede the child victim’s access to the regular court system or State-based non-judicial mechanisms, and that they provide child friendly information which is accessible, age appropriate and available in the language of the child about how to introduce complaints and seek redress through them.
9. States should require business enterprises that on their platform or within their service, there are easily accessible ways for any person, and in particular children, to report any material or activity which causes them concern and that adequate resources are devoted to ensure that reports received are dealt with efficiently and within reasonable timescales.
10. Notice and takedown procedures to remove illegal content from online networks as well as information about all remedies available at domestic and international level must be easily accessible, age-appropriate and available in the language of the child.
11. Mechanisms and processes in place should ensure that access to remedies is speedy and child-friendly, and provides appropriate redress to victims.
12. **National Frameworks** 
    1. *Legal framework*
13. States should review and, where necessary, update their legal framework to support the full realisation of the rights of the child in the digital environment. A comprehensive legal framework should address notably preventive measures, measures integrating digital environment childhood related issues integrated into public policies on support for parenting; prohibition of all forms of violence, exploitation and abuse of children in the digital environment; provision of effective remedies, recovery and reintegration to address violations of children’s rights; the establishment of child-sensitive counseling, reporting and complaint mechanisms; child-friendly mechanisms for consultation and participation; and accountability mechanisms to fight impunity.[[24]](#footnote-24)
14. States should ensure that the legal framework covers crimes that can be committed against a child in the digital environment, where possible formulated in a technology-neutral manner and which reflect the emergence of new technologies. Such crimes should include among others sexual exploitation and abuse, harassment, threats, and identity theft. Due account should be taken of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the Convention on Cybercrime and the Optional Protocol to the UNCRC on the sale of children, child prostitution and child pornography, which serve as benchmarks for criminal law reform and wider reform of services for victims and provide useful resources for informing the creation of an effective legislative framework. Such frameworks should include specific definitions of offences as well as provisions requiring punishment for criminalised behaviour, allowing for more effective prosecution of offenders and services for victims.
15. States should evaluate the overall effectiveness of data protection frameworks in respect of children’s personal information. These frameworks should provide for effective mechanisms to enable children to obtain rectification or erasure of their data if these have been processed contrary to the provisions of domestic law by state and other actors or when children withdraw their consent.[[25]](#footnote-25) Measures in place should enable a child or his or her legal representative to obtain the removal, deletion or correction of personal data created by the child or concerning the child which could compromise their dignity, physical and psychological integrity, or privacy or be otherwise detrimental to his or her rights. Upon request, relevant actors should remove or delete such content, within a reasonable short period of time.
16. States should create a clear and predictable legal and regulatory environment which supports businesses and other third parties to meet their responsibilities with respect to children’s rights in the digital environment throughout their operations and in all territories where their services are used by children.[[26]](#footnote-26)
17. States should provide in their internal law for the rights of child victims to compensation from the perpetrator(s) and guarantee compensation in accordance with the conditions of the national law. Where appropriate, consideration should be given to the establishment of funds for child victims‘ compensation or measures or programmes aimed at providing therapeutic or other support, which could be funded through the application of criminal or non-criminal sanctions, including monetary sanctions.
    1. *Policy and institutional frameworks*

*National action plan or strategy*

1. In order to achieve greater coordination and coherence on the range of public policy areas that are relevant for children’s rights in the digital environment, States should consider establishing a national strategy and/or action plan, and ensure that policies and measures adopted to address these aspects are consistent and mutually reinforcing.
2. A comprehensive and coordinated strategy or action plan should identify competent bodies with responsibility and authority to implement the actions set out therein, contain realistic and time-specific targets, be supported by adequate human and financial resources, and be based on current scientific knowledge, ongoing and sufficiently-resourced research and good practices.
3. All relevant actors should be engaged in a state’s national strategy or action plan’s design, implementation and evaluation. In particular, children should be heard and empowered to contribute, with their informed consent and according to their evolving capacity, to this multi-stakeholder action. Adequate resources should be made available to ensure children’s meaningful participation.
4. Methodologies should be developed to assess progress and evaluate actions foreseen by the action plan or strategy at all levels and by all stakeholders. Evaluations should be conducted on a regular basis with a view to identifying policies and measures that are appropriate and effective in promoting, respecting and fulfilling children’s rights in the digital environment.
5. Information on State’s strategy or action plan’s implementation should be widely disseminated.

*Policies and resources*

1. States’ policies should support educational, cultural and other institutional providers of beneficial resources for children to make these available to children in the digital environment.
2. States should develop within the national framework for child protection a comprehensive policy approach within which the digital environment is expressly addressed, and to which all relevant actors contribute.
3. States should consider developing policies, operational guidelines and codes of conduct to build awareness and support among business enterprises within their jurisdiction with respect to their role and impact on children’s rights, their responsibilities and co-operation with relevant actors[[27]](#footnote-27).
4. States should ensure that arrangements are in place or improved to implement screening processes and to provide advice, guidance and assistance to any agency or employer who recruits staff to work with children, including within an online environment. The purpose of the processes and advice, guidance and assistance would be to reduce the risk of individuals with an inappropriate interest in children being recruited or placed in any kind of position of trust vis-a-vis children who may be using their service.
5. States should allocate resources and provide adequate and continuous training for law enforcement staff, members of the judiciary and professionals working with and for children. Such training should enhance their skills and knowledge of children’s rights in the digital environment, the risks children face online, how to recognise the signals that a child may be a victim of online harm and what steps to take in response, including reporting online violence and abuse against children.[[28]](#footnote-28)

*Research*

1. States should ensure that policies and initiatives are informed by rigorous and up-to-date evidence about children’s experiences in the digital environment. Research should be conducted independently of relevant interests, and should be sufficiently detailed to differentiate children’s experiences by age, gender, socio-economic status and factors that render children vulnerable or resilient in the digital environment. The purpose would be to map existing digital opportunities and risks for children and to identify emerging trends so as to guide the targeting of policy and resources to ensure children’s wellbeing in the digital environment.

*Addressing risks and impact for the rights of the child*

1. States should require business enterprises to undertake child rights due diligence. This would ensure that business enterprises identify, prevent and mitigate their impact on children's rights and freedoms, including across their business relationships and within global operations.[[29]](#footnote-29) In this context, business enterprises should be required to develop and apply child-oriented industry policies, standards or codes of conduct, in particular with regard to non-discrimination, respect for privacy, data protection, commercial activities targeted at children and harmful content, and promotion of children’s rights to information, expression and participation, and that their implementation is regularly reviewed and evaluated.
2. States should require business enterprises to perform risk assessments with respect to children and children’s rights in relation to the digital technologies, products, services and policies for which they are responsible, and to update those at appropriate intervals. These should also be required to demonstrate they are taking reasonable and proportionate measures to manage and mitigate risks, and are taking reasonable and proportionate steps to enforce their own specified terms and conditions of service.
3. States should encourage the production by business enterprises of parental controls that can mitigate risks for children in the digital environment and, where appropriate, monitor standards applied so that they are not unduly restrictive or give a false sense of security.

*Institutional aspects, mechanisms and services*

1. States should ensure that domestic institutions responsible for guaranteeing human and children’s rights address within their mandate children’s rights in relation to the digital environment, including aspects related to educational curriculum and digital literacy, standards and technical guidance for the production of positive digital content and services of social, educational and cultural benefit to children, child-friendly mechanisms for consultation and participation. They should be able to receive, investigate and address complaints by children in a child-sensitive manner, ensure the child’s right to privacy, and the protection of victims, and undertake monitoring, follow-up and verification activities for child victims.
2. States should establish monitoring mechanisms for the investigation and redress of children’s rights violations, as well as strengthen regulatory agencies’ responsibility for the development of standards relevant to children’s rights in the digital environment and related guidance.[[30]](#footnote-30)
3. Competent authorities should establish accessible, safe, confidential, age-appropriate, child-friendly and effective counselling, reporting and complaint mechanisms, such as helplines, as a core dimension of the national child protection system, with appropriate links to child support services and law enforcement, and where appropriate in close co-operation with external stakeholders. This should include the provision of safe, child-friendly and confidential points of contact for children to report self-generated sexual content, to the relevant authorities[[31]](#footnote-31). Telecommunications companies should consider waiving costs for incoming calls to child helplines by means of toll-free numbers. [[32]](#footnote-32)
4. States should establish mechanisms, within the child protection system, to ensure access and provide adequate support and assistance for children victims of violence, exploitation and abuse occurring through the digital environment, including services to ensure the child’s physical, psychological and social recovery and reintegration, and prevent their re-victimisation.
5. States should ensure that appropriate sex offender treatment programmes are available for persons convicted of sexual offences involving children and that services are available to anyone concerned about the possibility of their committing a sexual crime involving a child, including in the digital environment.
   1. *Co-operation and coordination at national level*
6. States should pursue a comprehensive and coordinated multi-stakeholder approach informing and engaging all relevant actors, including national, regional and local authorities, especially law enforcement, educational and social service agencies, independent human rights institutions, professionals working for and with children, civil society, business enterprises, industry associations, researchers, families and children, in ways which are tailored to their roles and functions.
7. States should designate an authority or create a mechanism to coordinate actions to assess developments in the digital environment that might impact children’s rights, and ensure that their national policies adequately address such developments. This authority/mechanism should be evidence-based and include effective representation from children.
8. States should take appropriate measures to develop co-operation frameworks, procedures and processes between competent state authorities, civil society and business enterprises, taking into account their respective roles and responsibilities, capacities and resources.
9. Civil society actors, as key catalysts in promoting the human rights dimension of the information society, should be encouraged to actively monitor, evaluate and promote children’s skills, well-being and related information literacy and training initiatives, including actions undertaken by other actors.
10. States should encourage media providers to be attentive to their role as an important source of information and reference for children, parents and educators in relation to children’s rights in the digital environment.
11. **International co-operation and coordination**
12. States should be encouraged to ratify and implement instruments relevant to the promotion and protection of children’s rights in the digital environment. Such instruments include inter alia the Optional Protocols to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and on a communications procedure, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), the Convention on Cybercrime (ETS No. 185), the Convention on Action against Trafficking in Human Beings (CETS No. 197), and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).
13. States should co-operate with each other, in accordance with these guidelines and through application of relevant international and regional instruments and arrangements agreed on the basis of uniform or reciprocal legislation and internal laws, to the widest extent possible, for the purpose of promoting, protecting and fulfilling children’s rights in the digital environment. In particular, States should:
14. have an adequate legal basis for providing assistance and where appropriate should have in place treaties, arrangements or other mechanisms to enhance cooperation;
15. ensure that their competent authorities can rapidly, constructively and effectively use clear channels or mechanisms for the effective transmission and execution of requests for information and other types of assistance;
16. have clear and efficient processes for the prioritization and timely execution of requests;
17. not prohibit or place unreasonable or unduly restrictive conditions on the provision of assistance or co-operation.
18. States should support regional and international capacity building efforts to improve policy and operational measures to protect and fulfil children’s rights in the digital environment, including the pooling and sharing of successful education and awareness raising tools.
19. States should cooperate with a view to standardizing content classification among countries and across stakeholder groups to define what is appropriate and what is inappropriate for children in order to harmonize protective measures.
20. States should expedite action to ensure their law enforcement agencies can connect to and co-operate with the INTERPOL database that deals with child abuse images (ICSE).
21. States should take measures to strengthen law enforcement and international co-operation, including information sharing, to combat sexual exploitation of children, including in travel and tourism and the migration context, and to improve the efficacy and operational usefulness of the Interpol system for notifying cross-border movements of child sex offenders.
22. Recognising its wider role in relation to the management of the internet, States should actively engage with the Internet Corporation for Assigned Names and Numbers (ICANN) to press for the effective implementation of polices which will enhance or sustain children’s rights, in particular by ensuring that web addresses which self-evidently advertise or promote child sexual abuse material or images or any other offenses against children are identified and removed, as well as prevented from being registered.
23. To facilitate implementation of the guidelines, member states should strengthen, as appropriate, co-operation within relevant intergovernmental bodies, transnational networks and other international organisations, having particular regard to the speed at which cross-border requests for information or co-operative support are processed.

1. Article 3 UNCRC; United Nations Committee on the Rights of the Child, General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. [↑](#footnote-ref-1)
2. Council of Europe Strategy on Internet Governance (2016-2021), CM Declaration on Internet Governance Principles, principle 1 – Human Rights, Democracy and Rule of Law (2011), Netmundial (2014) “Rights that people have offline must also be protected online”. [↑](#footnote-ref-2)
3. Article 6 UNCRC. [↑](#footnote-ref-3)
4. Article 2 UNCRC. [↑](#footnote-ref-4)
5. Article 12 UNCRC. [↑](#footnote-ref-5)
6. United Nations Committee on the Rights of the Child, General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. [↑](#footnote-ref-6)
7. United Nations Committee on the Rights of the Child, General comment No. 20 (2016) on the implementation of the rights of the child during adolescence. [↑](#footnote-ref-7)
8. United Nations Committee on the Rights of the Child, General comment No. 20 (2016) on the implementation of the rights of the child during adolescence. [↑](#footnote-ref-8)
9. United Nations Committee on the Rights of the Child, *General Comment No. 5 (2003) General measures of implementation of the Convention on the Rights of the Child,* CRC/GC/2003/5. para.1 [↑](#footnote-ref-9)
10. UNCRC, Article 9, para. 3. [↑](#footnote-ref-10)
11. ## Article 9 United Nations Convention on the Rights of Persons with Disabilities.

    [↑](#footnote-ref-11)
12. UNCRC, Article 13. [↑](#footnote-ref-12)
13. European Court of Human Rights, Handyside v. UK. [↑](#footnote-ref-13)
14. # UNCRC, Article 17; Framework Convention for the Protection of National Minorities; **European Charter for Regional or Minority Languages.**

    [↑](#footnote-ref-14)
15. Article 10 European Convention on Human Rights and its case law. [↑](#footnote-ref-15)
16. UNCRC, article 16. [↑](#footnote-ref-16)
17. UNCRC, article 16, CM/Rec(2014)6 on a Guide to human rights for Internet users. [↑](#footnote-ref-17)
18. Article 6 Convention No. 108. [↑](#footnote-ref-18)
19. CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling [↑](#footnote-ref-19)
20. CM/Rec(2016)5 on Internet freedom, Article 8 of the ECHR [↑](#footnote-ref-20)
21. Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children to the Human Rights Council,* A/HRC/31/20 (January 2016), para. 103. [↑](#footnote-ref-21)
22. CM/Rec(2014)6 on a Guide to human rights for Internet users. [↑](#footnote-ref-22)
23. CM/Rec(2014)6 on a Guide to human rights for Internet users. [↑](#footnote-ref-23)
24. Special Representative of the Secretary-General on Violence against Children, *Releasing children’s potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), p. 55 [↑](#footnote-ref-24)
25. Article 8, STCE No. 108. [↑](#footnote-ref-25)
26. UN Committee on the Rights of the Child, *General Comment No. 16*, para. 53 [↑](#footnote-ref-26)
27. For example, see [Guidelines for the co-operation between law enforcement and service providers against cybercrime(2008)](https://rm.coe.int/16802fa3ba). [↑](#footnote-ref-27)
28. UNSRSG on violence (2014) Releasing children’s potential and minimising risks [↑](#footnote-ref-28)
29. UN Committee on the Rights of the Child, *General Comment No. 16*, para. 62 [↑](#footnote-ref-29)
30. UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 96 [↑](#footnote-ref-30)
31. Source: ICT and child exploitation – UN high commissioner for HR, A/HRC/34 [↑](#footnote-ref-31)
32. Source : UNSRSG on violence (2014) Releasing children’s potential and minimising risks [↑](#footnote-ref-32)