COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES Recommendations **CM/Rec(2018)7** 4 July 2018

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

(Adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies)

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 a 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;

Reaffirming the commitment of member States to ensure that every child enjoys the full range of human rights enshrined in the United Nations Convention on the Rights of the Child (UNCRC), in the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), and their protocols, and that these rights should be fully respected, protected and fulfilled, as technology continues to develop;

Having regard to the obligations and commitments as undertaken within other relevant international and European conventions, such as the revised European Social Charter (ETS No. 163), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), the Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), the Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197), the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), the Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210) and taking into account the recommendations, resolutions and declarations of the Committee of Ministers and of the Parliamentary Assembly of the Council of Europe in this field;

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

Conscious that information and communication technologies (ICTs) are an important tool in children's lives for education, socialisation, expression and inclusion, while at the same time their use can generate risks, including violence, exploitation and abuse;

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 Internet Governance Strategy (2016-2019), according to which the internet should be a safe, secure, open and enabling environment for everyone, children included, without discrimination;

Recognising that children are entitled to receive support and guidance in their discovery and use of the digital environment, respecting the rights and dignity of children and others;

Determined to contribute effectively to ensuring that consistent policies are being devised, with the participation of children, 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 the rights of the child are respected, protected and fulfilled;

Emphasising that States have the primary responsibility to respect, protect and fulfil the rights of the child, and reaffirming the rights, role and responsibility of parents or carers to provide, in a manner consistent with the best interests and evolving capacities of the child, appropriate direction and guidance for children to exercise their rights;

Recognising also that business enterprises have a responsibility to respect human rights, including the rights of the child, as affirmed in Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business, the United Nations Committee on the Rights of the Child's General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, the United Nations Guiding Principles on Business and Human Rights (2011), the Council of Europe Guidelines for the co-operation between law enforcement and internet service providers against cybercrime (2008), the Human Rights Guidelines for Internet service providers (Council of Europe and EuroISPA) (2008) and the Human Rights Guidelines for online games providers (Council of Europe and ISFE) (2008), and the Children's Rights and Business Principles (2012) drawn up by UNICEF, the UN Global Compact and the NGO Save the Children;

Conscious that policies in this area require a combination of public and private, legal and voluntary measures, that all relevant public and private stakeholders share responsibility for ensuring the rights of the child in the digital environment, and that co-ordination of their actions is necessary;

Taking into account the views and opinions of children consulted in member States of the Council of Europe;

Recognising the need to develop guidance to assist States and other relevant stakeholders in their efforts to adopt a comprehensive, strategic approach for respecting, protecting and fulfilling the rights of the child in the digital environment, rooted in the standards established by the UNCRC and the Council of Europe and underpinned by the meaningful participation of children,

Recommends that the governments of the member States:

1. review their legislation, policies and practice to ensure that they are in line with the recommendations, principles and further guidance set out in the appendix of this recommendation, promote their implementation in all relevant areas and evaluate the effectiveness of the measures taken at regular intervals, with the participation of relevant stakeholders;

2. ensure that this recommendation, including the guidelines in the appendix, is translated and disseminated as widely as possible among competent authorities and stakeholders, including parliaments, specialised public agencies and civil society organisations, as well as children, in a child-friendly manner and through accessible means, modes and formats of communication;

3. require business enterprises to meet their responsibility to respect the rights of the child in the digital environment and to take implementing measures, and encourage them to co-operate with relevant State stakeholders, civil society organisations and children, taking into account relevant international and European standards and guidance;

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

5. examine the implementation of this recommendation and the guidelines in its appendix within the Committee of Ministers and with the participation of relevant stakeholders every five years at least and, if appropriate, at more frequent intervals.

Appendix to Recommendation CM/Rec(2018)7

Guidelines to respect, protect and fulfil the rights of the child in the digital environment

1. Purpose and scope

International and European binding instruments and standards set out obligations or provide benchmarks for member States to respect, protect and fulfil the human rights and fundamental freedoms of children in the digital environment. 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.

The present guidelines are intended to provide assistance to relevant stakeholders in the implementation of the rights enshrined in international and European human rights conventions and standards, in the light of the case law of the European Court of Human Rights. They seek in particular to:

a. guide States in formulating legislation, policies and other measures to promote the realisation of the full array of the rights of the child in the digital environment and address the full range of ways in which the digital environment affects children's well-being and enjoyment of human rights;
b. promote the devising, implementation and monitoring by States of a comprehensive strategic and co-ordinated approach, reflecting the principles contained in the present guidelines;
c. ensure that States require business enterprises and other relevant stakeholders to meet their responsibility to respect the rights of the child in the digital environment and encourage them to support and promote these rights;
d. ensure concerted action and co-operation at national and international level to respect, protect and fulfil the rights of the child in the digital environment.

For the purpose of this text:

– "child" refers to any person under the age of 18 years;

– "digital environment" is understood as encompassing information and communication technologies (ICTs), including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services.

2. Fundamental principles and rights

The principles and rights set out below should be read as applying to all sections of these guidelines.

2.1. Best interests of the child

1. In all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration. 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 information as well as participation rights.

2.2. Evolving capacities of the child

2. The capacities of a child develop gradually from birth to the age of 18. Moreover, individual children reach different levels of maturity at different ages. States and other relevant stakeholders should recognise the evolving capacities of children, including those of children with disabilities or in vulnerable situations, 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 fulfil the rights of adolescents may differ significantly from those adopted for younger children.

2.3. Right to non-discrimination

3. The rights of the child apply to all children without discrimination on any grounds. All rights are to be granted without discrimination of any kind, irrespective of the child's age, and the child's or his or her parents' or legal guardians' race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth,[1] or other status.

4. Whereas efforts should be undertaken to respect, protect 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 children's vulnerability and to empower, protect and support them.

2.4. Right to be heard

5. Children have the right to express themselves freely in all matters affecting them, and their views should be given due weight in accordance with their age and maturity.

6. States and other relevant stakeholders should provide children with information on their rights, including their participation rights, in a way they can understand, and which is appropriate to their maturity and circumstances. They should enhance opportunities for them to express themselves through ICTs as a complement to face-to-face participation. Children should be informed of mechanisms and services providing adequate support, and of procedures for complaints, remedies or redress should their rights be violated. Such information should also be made available to their parents or carers to enable them to support children in exercising their rights.

7. Furthermore, States and other relevant stakeholders should actively engage children to participate meaningfully in devising, implementing and evaluating legislation, policies, mechanisms, practices, technologies and resources that aim to respect, protect and fulfil the rights of the child in the digital environment.

2.5. Duty to engage other stakeholders

8. In accordance with relevant international standards, States have the primary obligation to respect, protect and fulfil the rights of every child within their jurisdiction and must engage all relevant stakeholders, in particular educational and child protection and care systems, public institutions and business enterprises, civil society stakeholders, as well as children themselves and their parents, legal guardian or any other person who takes care of the child, in order to effectively implement these obligations.

9. Concerning the digital environment, each State should apply such measures as may be necessary to require that business enterprises meet their responsibility to respect the rights of the child in all their operations within the State's jurisdiction, and, as appropriate, in all their operations abroad when domiciled in its jurisdiction. Furthermore, States should encourage and support by other relevant means business enterprises in understanding and respecting the rights of the child.

3. Operational principles and measures to respect, protect and fulfil the rights of the child in the digital environment

3.1. Access to the digital environment

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

11. States should make appropriate arrangements to ensure that all children have adequate, affordable and secure access to devices, connectivity, services and content which is specifically intended for children. Insofar as this is possible, in dedicated public spaces, States should take measures to render access to the digital environment free of charge.

[1] United Nations Convention on the Rights of the Child, Article 2.1.

12. 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 alternative care, children deprived of liberty or whose parents are deprived of liberty, children in the context of international migration, children in street situations and children in rural communities. In particular, States should require online service providers to ensure that their services are accessible by children with disabilities.

13. Connectivity and access to devices, services and content should be 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.

14. 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 online services or content are accessible, fair, transparent, intelligible, available in the child's language and formulated in clear, child-friendly and age-appropriate language where relevant.

15. States should ensure a plurality of sources of high-quality information and educational digital content and services for children. Children's rights should be taken into account in related public procurement procedures, for instance for educational tools, so that access to and use of digital services and content is not unduly restricted by commercial interests or filters.

3.2. Right to freedom of expression and information

16. 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. States should take measures to guarantee children's right to hold and express any views, opinions or expressions on matters of importance to them, through the media of their choice, and irrespective of whether or not their views and opinions are received favourably by the State or other stakeholders.

17. Children, as creators and distributors of information in the digital environment, should be made aware by States, especially through educational programmes, of how to exercise their right to freedom of expression in the digital environment while respecting the rights and dignity of others, including other children. In particular, such programmes should address aspects such as freedom of expression and legitimate restrictions thereon, for example to respect intellectual property rights or prohibit incitement to hatred and violence.

18. States should initiate and encourage the provision of diverse high-quality online content and services of social and cultural benefit to children in support of their fullest development and participation in society. This should include the largest possible amount of high-quality content that is specifically made for children, easy for them to find and understand, provided in their language, and which is adapted to their age and maturity. In this context, information on the rights of the child, including in the digital environment; news; health; information on sexuality, among other resources of benefit to them, is particularly important. In particular, States should ensure that children are able to locate and explore public service media and high-quality content likely to be of benefit to them.

19. Where States make provision for 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, media online.

20. Any restrictions on children's right to freedom of expression and information in the digital environment should comply with international and European human rights conventions and standards. States should take measures to ensure that children are informed of restrictions in place, such as content filtering, in a manner appropriate to their evolving capacities, and that they are provided with guidance on appropriate remedies, including on how and to whom to make a complaint, report an abuse or request help and counselling. Where appropriate, parents or carers should also be informed of such restrictions and appropriate remedies.

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

21. The digital environment provides distinctive opportunities for the rights of the child to participate, to engage in play and to peaceful assembly and association, including through online communication, gaming, networking and entertainment. States should co-operate with other stakeholders to provide for access of children to such activities that can foster participation, inclusion, digital citizenship and resilience both online and offline.

22. Recognising children's right to engage in play and recreational activities appropriate to their age and maturity, 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, artistic, cultural, educational and recreational benefit to all children. This includes interactive and play-based tools that stimulate skills such as creativity, teamwork and problem solving, appropriate to their evolving capacities and with particular attention to the needs of children in vulnerable situations. Where children participate in the creation or production of these tools, measures should be in place to protect the child's intellectual property rights.

23. States should provide children with information appropriate to their age and maturity, including in non-written forms and through social networking and other media, on their rights, in particular their participation rights. States should also inform them of the opportunities available to them, and where they can get support to take advantage of these opportunities.

24. States should take measures to ensure that children are able to participate effectively in local, national and global public-policy and political debates and to support the development of online civic and social platforms to facilitate their participation and their enjoyment of the right to assembly and association, strengthening their capacity for democratic citizenship and political awareness. States should also ensure that children's participation in the digital environment is acted upon meaningfully, building on existing good practice for child participation and available tools for assessment.

25. States should take measures to protect children exercising their right to peaceful assembly and association in the digital environment from monitoring and surveillance, whether carried out by State authorities directly or in collaboration with private sector entities. Where such measures interfere with the exercise by children of their rights, they should be subject to conditions and safeguards against abuse, in line with international and European human rights conventions and standards. Notably, they should be prescribed by a law which is accessible, precise, clear and foreseeable, pursue a legitimate aim, be necessary in a democratic society and proportionate to the legitimate aim pursued, and allow for effective remedies.

3.4. Privacy and data protection

26. Children have a right to private and family life in the digital environment, which includes the protection of their personal data and respect for the confidentiality of their correspondence and private communications.

27. States must respect, protect and fulfil the right of the child to privacy and data protection. States should ensure that relevant stakeholders, in particular those processing personal data, but also the child's peers, parents or carers, and educators, are made aware of and respect the child's right to privacy and data protection.

28. States and other stakeholders should ensure that children are made aware of how to exercise their right to privacy and data protection, taking into account their age and maturity and, where appropriate, with the direction and guidance of their parents, carers, legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child.

29. Recognising that personal data can be processed to the benefit of children, States should take measures to ensure that children's personal data is processed fairly, lawfully, accurately and securely, for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents, carer or legal representative, or in accordance with another legitimate basis laid down by law. The data minimisation principle should be respected, meaning that the personal data processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

30. Where States take measures to decide upon an age at which children are considered to be capable of consenting to the processing of personal data, their rights, views, best interests and evolving capacities must be taken into consideration. This should be monitored and evaluated while taking into account children's actual understanding of data collection practices and technological developments. When children are below that age and parental consent is required, States should require that reasonable efforts are made to verify that consent is given by the parent or legal representative of the child.

31. States should ensure that the likely impact of intended data processing on the rights of the child is assessed and that the data processing is designed to prevent or minimise the risk of interference with those rights.

32. States should ensure that the processing of special categories of data which are considered sensitive, such as genetic data, biometric data uniquely identifying a child, personal data relating to criminal convictions, and personal data that reveal racial or ethnic origins, political opinions, religious or other beliefs, mental and physical health, or sexual life, should in all instances only be allowed where appropriate safeguards are enshrined in law.

33. States should ensure that easily accessible, meaningful, child-friendly and age-appropriate information about privacy tools, settings and remedies is made available to children. Children and/or their parents or carers or legal representatives should be informed by a data controller how their personal data is being processed. This should include information for instance on how data is collected, stored, used and disclosed, on their rights to access their data, to rectify or erase this data or object to its processing, and how to exercise their rights.

34. States should ensure that children and/or their parents, carers or legal representative have the right to withdraw their consent to the processing of their personal data, have access to their personal data and to have it rectified or erased, notably when the processing is unlawful or when it compromises their dignity, safety or privacy.

35. In relation to the processing of children's personal data, States should implement, or 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 strong safeguards for the right to privacy and data protection into devices and services.

36. With respect to connected or smart devices, including those incorporated in toys and clothes, States should take particular care to ensure that data-protection principles, rules and rights are also respected when such products are directed principally at children or are likely to be regularly used by or in physical proximity to children.

37. Profiling of children, which is any form of automated processing of personal data which consists of applying a "profile" to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes, should be prohibited by law. In exceptional circumstances, States may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law.

38. Children shall not be subjected to arbitrary or unlawful interference with their privacy in the digital environment. Measures which may restrict children's right to privacy 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. Surveillance or interception measures in particular must comply with these conditions and should be subject to effective, independent and impartial oversight.

39. States should not prohibit in law or practice anonymity, pseudonymity or the usage of encryption technologies for children.

3.5. Right to education

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

Digital literacy

41. States should promote the development of digital literacy, including media and information literacies and digital citizenship education, to ensure that children have the competence to engage in the digital environment wisely and the resilience to cope with its associated risks. Digital literacy education should be included in the basic education curriculum from the earliest years, taking into account children's evolving capacities.

42. In support of a wide range of rights of the child, digital literacy education should include the technical or functional competences to use a wide range of online tools and resources, as well as skills related to content creation and the critical understanding of the digital environment, its opportunities and risks.

43. Digital literacy should be effectively promoted in the settings where children use the internet, especially schools and organisations working with and for children. States should also promote and support the digital literacy of parents or carers through the State's established mechanisms for reaching parents as an essential means of creating a safer and sustainable digital environment for children and families.

44. Recognising the potential advantages of educational policies that use digital networks to connect formal and non-formal learning, including at home, States should ensure that this does not disadvantage children who lack resources at home or live in residential institutions.

45. Particular efforts should be made by States and other relevant stakeholders, through the education and cultural system, to support and promote the digital literacy of children who have little or no access to digital technology for socio-geographical or socio-economic reasons, as well as sometimes for reasons of place of residence and also of children who have access to but do not use digital technology, who lack the skills to use or underuse digital technology for reasons of vulnerability, in particular for children with disabilities.

46. States should also make efforts to enhance the use of information and communication technology by girls and to promote the equality of opportunities and outcomes for all children.

Educational programmes and resources

47. States should ensure that sufficient high-quality educational resources, physical devices and infrastructures are available to benefit children's operation in the digital environment and support their formal, non-formal and informal education. These may be developed and distributed in co-operation with other relevant stakeholders. Such provision should be evaluated according to current good practice and necessary actions taken by States and other stakeholders to maintain high standards of education relevant to the digital environment.

48. States should develop and strengthen education and awareness-raising initiatives and programmes and user tools for children, parents or carers, and educators and volunteers working with children, with the involvement of children. Such programmes should include knowledge on preventive measures, on rights and responsibilities in the digital environment, identification and reporting of violations, remedies and available redress. Specifically, such programmes should teach children to understand, as appropriate according to their age and evolving capacities, what it means to give consent, to respect other fundamental rights, their own and those of others, to seek redress when needed and to use available tools to protect and fulfil their rights in the digital environment. Furthermore, they should enable children to understand and deal

with potentially harmful content (such as violence and self-harm, adult pornography, child sexual abuse material, discrimination and racism, hate speech) and behaviour (such as the solicitation of children for sexual purposes or "grooming", bullying or harassment, unlawful processing of personal data, violation of intellectual property rights), and potential consequences of the way in which information about children or shared by children might be further disseminated in different settings and by others.

49. Formal and non-formal educational and cultural institutions (including archives, libraries, museums, child and youth-led organisations, and other learning institutions) should be supported and encouraged to develop and make available a variety of digital and interactive learning resources and to co-operate across institutional boundaries to optimise learning opportunities in relation to the digital environment.

3.6. The right to protection and safety

50. Taking into account the development of new technologies, children have the right to be protected from all forms of violence, exploitation and abuse in the digital environment. Any protective measures should take into consideration the best interests and evolving capacities of the child and not unduly restrict the exercise of other rights.

51. There are a number of areas of concern for children's healthy development and well-being which may arise in connection with the digital environment, including but not limited to, risks of harm from:

- sexual exploitation and abuse, solicitation for sexual purposes (grooming), online recruitment of children for the commission of criminal offences, for participation in extremist political or religious movements or for trafficking purposes (contact risks);
- the degrading and stereotyped portrayal and over-sexualisation of women and children in particular; the portrayal and glorification of violence and self-harm, in particular suicides; demeaning, discriminatory or racist expressions or apologia for such conduct; advertising, adult content (content risks);
- bullying, stalking and other forms of harassment, non-consensual dissemination of sexual images, extortion, hate speech, hacking, gambling, illegal downloading or other intellectual property infringements, commercial exploitation (conduct risks);
- excessive use, sleep deprivation and physical harm (health risks).

All of the above factors are capable of adversely affecting the physical, emotional and psychological well-being of a child.

Measures to address risks in the digital environment

52. Being mindful of the speed at which new technologies can emerge, States should take precautionary measures, including by assessing on a regular basis any risks of harm that these may pose to children's health, despite the absence of certainty at that time with regard to scientific and technical knowledge of the existence or extent of such risks.

53. States should promote and provide incentives to business enterprises to implement safety by design, privacy by design and privacy by default as guiding principles for products and services' features and functionalities addressed to or used by children.

54. Where States encourage the development, production and regular update by business enterprises of parental controls to mitigate risks for children in the digital environment, they should ensure that such controls are developed and deployed taking into account children's evolving capacities, and that they do not reinforce discriminatory attitudes, infringe children's right to privacy or deny children the right to information, in accordance with their age and maturity.

Protection and awareness-raising measures

55. Specific measures and policies should be adopted to protect infants from premature exposure to the digital environment due to limited benefits with respect to their particular physical, psychological, social and stimulation needs.

56. States should require the use of effective systems of age-verification to ensure children are protected from products, services and content in the digital environment which are legally restricted with reference to specific ages, using methods that are consistent with the principles of data minimisation.

57. States should take measures to ensure that children are protected from commercial exploitation in the digital environment, including exposure to age-inappropriate forms of advertising and marketing. This includes ensuring that business enterprises do not engage in unfair commercial practices towards children, requiring that digital advertising and marketing towards children is clearly distinguishable to them as such, and requiring all relevant stakeholders to limit the processing of children's personal data for commercial purposes.

58. States are encouraged to co-operate with the media, with due respect for media freedom, with educational institutions and other relevant stakeholders, to develop awareness-raising programmes aimed at protecting children from harmful content as well as preventing their involvement in illegal online activities.

59. States should take measures to encourage business enterprises and other relevant stakeholders to develop and implement policies that address cyberbullying, harassment and incitement to hatred and violence in the digital environment. Such policies should include clear information on unacceptable behaviour, reporting mechanisms and meaningful support for children involved in such acts.

60. States should share good practices on ways to address risks in the digital environment, in relation to both prevention and remedies. States should put in place public awareness-raising measures about counselling, reporting and complaint mechanisms.

Measures regarding child sexual abuse material

61. Policing with respect to child sexual abuse material should be victim-focused with the highest priority being given to identifying, locating, protecting and providing rehabilitative services to the child depicted in such materials.

62. States should continually monitor whether and how child sexual abuse materials are hosted within their jurisdiction and require law-enforcement authorities to establish databases of "hashes",[2] with a view to expediting actions to identify and locate children subjected to sexual exploitation or abuse and apprehending perpetrators.

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

64. Mindful of available technologies and without prejudice to the principles of liability of internet intermediaries and their exemption from general monitoring obligations, 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, for example in relation to the production, distribution, provision of access to, advertising of or storage of child sexual abuse material or other forms of online child abuse.

65. States should require relevant business enterprises to apply hash lists with a view to ensuring that their networks are not being misused to store or distribute child sexual abuse images.

66. States should require that business enterprises and other relevant stakeholders take promptly all necessary steps to secure the availability of metadata concerning any child sexual exploitation and abuse material found on local servers, make them available to law-enforcement authorities, remove these materials and, pending their removal, restrict access to such materials found on servers outside of their jurisdiction.

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

3.7. Remedies

67. Member States should ensure the effective implementation of their obligations under Articles 6 and 13 of the European Convention on Human Rights (ETS No. 5), and other international and European human rights instruments, to fulfil a child's right to an effective remedy when their human rights and fundamental freedoms have been infringed in the digital environment. This entails the provision of available, known, accessible, affordable, and child-friendly avenues through which children, as well as their parents or legal representatives, may submit complaints and seek remedies. Effective remedies can include, depending on the violation in question, inquiry, explanation, reply, correction, proceedings, immediate removal of unlawful content, apology, reinstatement, reconnection and compensation.

68. Children should be provided with information and advice about remedies available at domestic level in a manner adapted to their age and maturity, in a language which they can understand and which is gender and culture sensitive. Mechanisms and processes in place should ensure that access to remedies is speedy and child-friendly, and provides appropriate redress to children.

69. States should ensure that in all cases access to courts or judicial review of administrative remedies and other procedures are available, in line with the principles set out in the Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice (2010).

70. States should, where appropriate, also provide children and/or their parents or legal representatives with non-judicial mechanisms, administrative or other means to seek remedy, such as through ombudspersons for children and other national human rights institutions and data-protection authorities. The availability, adequacy and effectiveness of these mechanisms for handling cases of violations or abuses of the rights of the child in the digital environment should be reviewed on a regular basis.

71. States, as the primary responsible entity, should take appropriate steps to protect children against human rights abuses within the digital environment by business enterprises and to ensure that children have access to an effective remedy, including by:

a. implementing policies and measures to encourage business enterprises to establish their own remedial and grievance mechanisms, in line with the effectiveness criteria set out in the UN Guiding Principles on Business and Human Rights, while ensuring that these mechanisms do not impede the child's access to the State-based judicial or non-judicial mechanisms;
b. encouraging business enterprises to provide information which is accessible, age-appropriate and available in the language of the child about how to introduce complaints and seek redress through remedial and grievance mechanisms;
c. requiring that business enterprises make available, on their platform or within their service, easily accessible ways for any person, and in particular children, to report any material or activity which causes them concern and that reports received are dealt with efficiently and within reasonable timescales.

4. National frameworks

4.1. Legal framework

72. Laws and policies related to the digital environment should be assessed, at their drafting stage, with regard to the impact that their implementation may have on children's enjoyment of human rights and fundamental freedoms. States should review at regular intervals, and, where necessary, update legal frameworks to support the full realisation of the rights of the child in the digital environment.

73. A comprehensive legal framework should provide for preventive and protective measures in relation to the digital environment; provide support measures for parents and carers; prohibit all forms of violence, exploitation and abuse; include effective remedies, recovery and reintegration services; establish child and

gender-sensitive counselling, reporting and complaint mechanisms; encompass child-friendly mechanisms for consultation and participation; and set up accountability mechanisms to fight impunity.

74. States should ensure that their legal frameworks encompass the full range of unlawful acts which can be committed in the digital environment, where possible formulated in a technology-neutral manner, leaving room for the emergence of new technologies. Such frameworks should include definitions of offences, criminal, civil or administrative liability and sanctions for natural and legal persons, and provisions of services for children. Due account should be taken of relevant instruments, such as the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), the Convention on Cybercrime (ETS No. 185) and the Optional Protocols to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000) and on a communications procedure (2011), which can serve as benchmarks for criminal law reform and wider reform of legal frameworks and services and can inform the development of an effective legislative framework.

75. Where forms of peer-to-peer online violence or abuse breaches occur, States should, as far as possible, pursue suitable and adequate preventive and restorative approaches, while preventing the criminalisation of children.

76. States should set up legal frameworks that apply to the processing of personal data of children and regularly evaluate the overall effectiveness of such frameworks. Due account should be taken of the relevant international and European instruments which refer to data-protection principles and rights, such as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

77. Legal frameworks in place should provide that independent data-protection authorities are competent to address complaints made by children and/or their parents or carers or legal representatives related to the unlawful processing of personal data of children and establish effective mechanisms which enable children to seek rectification or erasure of their data if these have been processed contrary to the provisions of domestic law or when children withdraw their consent. Upon request, relevant public and private stakeholders should be obliged to expediently remove or delete such content free of charge.

78. States should create a clear and predictable legal and regulatory environment which helps businesses and other stakeholders meet their responsibility to respect the rights of the child in the digital environment throughout their operations.

79. States should ensure that children or their legal representatives can seek compensation from perpetrator(s) for violations of their rights and abuses. Where appropriate, consideration should be given to the establishment of funds for the compensation of child victims or measures or programmes aimed at providing therapeutic or other support.

Specific requirements for the registry for a country code top-level domain

80. When awarding a contract or licence to an entity to become the registry for a country code top-level domain, States should include clear requirements 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 on any domain within the registry's purview and the establishment by the registry of mechanisms to ensure that this policy is enforced, including by registrars and registrants. The same requirements should apply to the registration of generic top-level domains.

81. Where a registrant proposes to establish or renew a site or service targeted at children or used by children in substantial numbers within their country code domain, States should ensure that the registry or other competent authority requires registrants to put in place appropriate child-protection policies. This may include, for example, requiring that neither the registrant nor anyone employed by the registrant in connection with delivering the service or in managing any data generated by the service has been convicted of acts of sexual exploitation or sexual abuse of children or other relevant offences.

4.2. Policy and institutional frameworks

Overall strategy and policy coherence

82. In order to achieve greater co-ordination and policy coherence across the full range of the rights of the child in the digital environment, States should establish a comprehensive strategic national approach, and ensure that policies and measures are consistent and mutually reinforcing. This may include the adoption of a strategy or action plan or the integration of specific attention to the rights of the child in the digital environment into existing action plans, strategies and policies in a consolidated manner.

83. A comprehensive strategic national approach should identify competent bodies with the 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.

84. States should engage all relevant stakeholders, such as ombudspersons for children and other independent human rights institutions, education stakeholders, data-protection authorities, business enterprises and civil society, including child and youth-led organisations, in the design, drafting, implementation and evaluation of a national strategy or action plan. In particular, States should ensure that children are consulted and empowered to contribute to these processes, with their informed consent and according to their evolving capacities. Due weight should be given to children's views. Children should be informed about how their views were taken into account and how these views influenced the decision-making process. Adequate resources should be made available to ensure children's meaningful participation.

85. Methodologies should be developed to assess progress and evaluate actions foreseen by the national strategy or action plan 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 respecting, protecting and fulfilling the rights of the child in the digital environment.

86. States should take appropriate measures to widely disseminate information on adopted strategies or action plans and their implementation.

Sectoral policies

87. States should ensure that policies and initiatives are informed by rigorous and up-to-date evidence about children's experiences in the digital environment, in order to map existing opportunities and risks for children, identify emerging trends and guide the targeting of policy and resources to ensure children's well-being in the digital environment.

88. States should devise and implement policies that support educational, cultural and other institutional providers of beneficial resources for children to make these available to children, parents and carers in the digital environment.

89. States should strengthen regulatory agencies' responsibility for drawing up, implementing and enforcing standards and guidance relevant to the rights of the child in the digital environment.

90. States should take measures, including the drafting of policies, operational guidelines and/or codes of conduct, to build awareness and support among business enterprises within their jurisdiction regarding their roles, responsibilities and impact on the rights of the child, and their co-operation with relevant stakeholders.

91. States should devise, within the national framework for child protection, a comprehensive protection and safety policy within which the digital environment is expressly addressed and to which all relevant stakeholders contribute, including children. Such a policy should take into account existing standards and guidance, such as the Council of Europe Policy Guidelines on integrated national strategies for the protection of children from violence (2009).[3]

[3] Recommendation CM/Rec(2009)10 of the Committee of Ministers to member States on integrated national strategies for the protection of children from violence, Appendix 1.

92. States should put in place strategies to prevent their citizens' access to child sexual abuse material physically located in other jurisdictions, according to their own legislation or a set of internationally recognised criteria.

93. States should engage business enterprises and other relevant stakeholders in the implementation of their sectoral policies, notably the protection and safety policy framework and related awareness-raising measures.

Addressing the risks and impact for the rights of the child

94. States should require business enterprises and other stakeholders to undertake due diligence in order to identify, prevent and mitigate their impact on the rights of the child in the digital environment.

95. States should require business enterprises to perform regular child-rights risk assessments in relation to digital technologies, products, services and policies and to demonstrate that they are taking reasonable and proportionate measures to manage and mitigate such risks.

96. States should encourage business enterprises to develop, apply and regularly review and evaluate child-oriented industry policies, standards and codes of conduct to maximise opportunities and address risks in the digital environment.

97. Recognising that parents, carers and others may rely on an online service's stated terms and conditions of service as a guide to the suitability of that service for their child, being mindful of available technologies and without prejudice to the liability of internet intermediaries, States should require business enterprises to take reasonable, proportionate and effective measures to ensure that their terms and conditions of service are enforced.

Institutional aspects, mechanisms and services

98. States should ensure that institutions responsible for guaranteeing human and children's rights address within their mandate the rights of the child in relation to the digital environment, for example through the promotion of digital literacy skills, high-quality standards for the production of digital content and services of social, educational and cultural benefit to children and child-friendly mechanisms for consultation and participation.

99. States should ensure that there are institutions or mechanisms responsible to receive, investigate and address complaints from children and their parents or legal representatives about human rights violations or abuses in relation to the digital environment, employing child-sensitive procedures that ensure the child's right to privacy throughout and provide for monitoring and follow-up.

100. Competent authorities should establish accessible, safe, confidential, age-appropriate and gender-sensitive counselling, reporting and complaint mechanisms, for example through public bodies, hotlines, helplines and zero-rate chat applications managed by child helplines, and online platforms, as a core dimension of the national child-protection system, with appropriate links to child support services and law-enforcement authorities, and, where appropriate, in close co-operation with external stakeholders. This should include the provision of safe, child-friendly, free-of-charge points of contact for children to report violence, exploitation and abuse in the digital environment to the relevant authorities. Such mechanisms should ensure the child or their parents' or legal representatives' right to confidentiality and anonymity.

101. States should encourage telecommunications companies to waive costs for incoming calls to child helplines by means of toll-free telephone numbers.

102. States should ensure there is an effective mechanism to allow any person to report anonymously the existence of suspected illegal material online, in particular child sexual abuse material.

103. States should, as part of the child-protection system, ensure access to and provide adequate and gender-sensitive support services and assistance for children whose rights and privacy have been violated or who have been subjected to violence, sexual exploitation or abuse in the digital environment, including

services to ensure the child's physical and psychological recovery and social reintegration, and prevent their re-victimisation.

104. States should ensure that appropriate sex-offender treatment programmes are available for persons convicted of sexual offences involving children in the digital environment, and that services are made available to anyone concerned about the possibility of their committing a sexual crime involving a child, including in the digital environment.

Investment, resources and training

105. States should invest in hardware, software, connectivity, adequate bandwidth and teacher training in schools to support learning.

106. States should ensure that initial and in-service training informs and empowers educators so that they can support children in acquiring the skills and literacy needed to exercise their rights in the digital environment.

107. States should ensure that policies and measures provide educational institutions with the resources, training and support needed to take preventive and protective measures concerning children, including in school, against violence and abuses of digital media, in ways that prevent escalation, provide appropriate support to children affected by and involved in such acts, provide redress and build resilience.

108. States should take measures to ensure that adequate arrangements are in place to implement screening processes and to provide guidance, advice and assistance to any agency or employer who recruits staff or volunteers to work with children, including within the digital environment, in order to prevent and reduce the risk of individuals with a criminal record being recruited or placed in a position of trust vis-à-vis children.

109. States should allocate adequate resources and provide initial 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 the rights of the child in the digital environment, the risks children face online, how to recognise the signals that a child may be a victim of online harm, violence, abuse and exploitation and what steps to take in response.

110. States should invest in research and knowledge development, including child and youth participation in the field of the rights of the child in the digital environment. Research should be conducted independently of relevant interests and should be sufficiently detailed to differentiate children's experiences by age, sex, socio-economic status and other factors that render children vulnerable or resilient in the digital environment.

4.3. Co-operation and co-ordination at national level

111. States should pursue a comprehensive strategic and co-ordinated multi-stakeholder approach informing and engaging all relevant stakeholders, including national, regional and local law-enforcement and other authorities, educational and social-service agencies, independent human rights institutions, data-protection authorities, professionals working for and with children, civil society, including child and youth-led organisations, business enterprises, industry associations, researchers, families and children, in ways which are tailored to their roles and functions.

112. States should designate an authority or create a co-ordinating mechanism to assess developments in the digital environment that might impact the rights of the child and which includes children in its decision-making processes, and ensure that their national policies adequately address such developments.

113. States should set up co-operation frameworks, procedures and processes between competent State authorities, independent authorities, civil society and business enterprises, taking into account their respective roles and responsibilities, capacities and resources.

114. States should require platforms or providers of communication services to take prompt and effective action in response to complaints of peer-to-peer or other online violence or abuse and to co-operate with national authorities.

115. States should engage business enterprises, such as internet service providers and social network providers, to play an active role in preventing and deleting illegal content, as determined by law or by a judicial or other competent authority.

116. States should encourage civil society stakeholders, as key catalysts in promoting the human rights dimension of the digital environment, to actively monitor, evaluate and promote children's skills, well-being and related information literacy and training initiatives, including actions undertaken by other stakeholders, and to disseminate their findings and results.

117. States should encourage all professional media outlets, and public service media in particular, to be attentive to their role as an important source of information and reference for children, parents or carers, and educators in relation to the rights of the child in the digital environment, with due regard to international and European standards on freedom of expression and information and freedom of the media.

5. International co-operation and co-ordination

118. States should be encouraged to ratify and implement international instruments relevant to the promotion and protection of the rights of the child in the digital environment. Such instruments include, *inter alia*: the Optional Protocols to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000), and on a communications procedure (2011), 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) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), the Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197), and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

119. States should co-operate with each other by applying relevant international and regional instruments and arrangements, to the widest extent possible, for the purpose of respecting, protecting and fulfilling the rights of the child in the digital environment. In particular, they should:

a. have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enable efficient co-operation with other States;
b. 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;
c. have clear and efficient processes for the prioritisation and timely execution of requests;
d. not prohibit or place unreasonable or unduly restrictive conditions on the provision of assistance or co-operation.

120. States should support regional and international capacity-building efforts to improve policy and operational measures to respect, protect and fulfil the rights of the child in the digital environment, including the pooling and sharing of successful education and awareness-raising tools.

121. States should co-operate with a view to promoting standardisation of content classification and advisory labels among countries and across stakeholder groups to define what is appropriate and what is inappropriate for children.

122. States should expedite action to ensure that their law-enforcement agencies can connect to the INTERPOL database that deals with child sexual abuse material.

123. 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 policies which will enhance or sustain the rights of the child, in particular by ensuring that web addresses which self-evidently advertise or promote child sexual abuse material or any other offences against children are identified and removed, or not authorised to be registered.

124. To facilitate implementation of these guidelines, member States should strengthen co-operation within relevant intergovernmental bodies, transnational networks and other international organisations.