

**Children's Rights in the Digital Environment:
European Network of Ombudspersons for
Children (ENOC) Member Questionnaire
Findings**

Results Report

September 2019

Introduction

In 2019 the theme of ENOC’s Statement was agreed as children’s rights in the digital environment. The purpose of ENOC’s annual Statement is to make recommendations which will support the respect, promotion and fulfilment of children’s rights with regard to the United Nations Convention on the Rights of the Child and its founding principles.

In order to ensure that the Statement fully reflects the experiences, views and advice of ENOC membership, a questionnaire was distributed to Members to inform the Statement drafting process. The content of the questionnaire drew on the principles and measures outlined in the Recommendation of the Committee of Ministers to member States on guidelines to respect, protect and fulfil the rights of the child in the digital environment (CM/Rec(2018)7). This document provides an overview of the range of protections and positive measures which ENOC Members report are currently in place as well as those areas where improvement is needed in order to properly respect promote and fulfil children’s rights in the digital environment.

Overview of Responses

In total 26 Members¹ responded to the survey and as the table below shows this included a good response from Eastern European, Scandinavian and Mediterranean countries. Two of the four jurisdictions of the UK responded, as did Ireland.

Albania	Malta
Azerbaijan	Montenegro
Belgium (Flemish Region)	Netherlands
Bosnia-Herzegovina	Northern Ireland
Cyprus	Norway
Denmark	Poland
Estonia	Serbia
Finland	Slovakia
France	Spain (Basque Country)
Ireland	Spain (Catalonia)

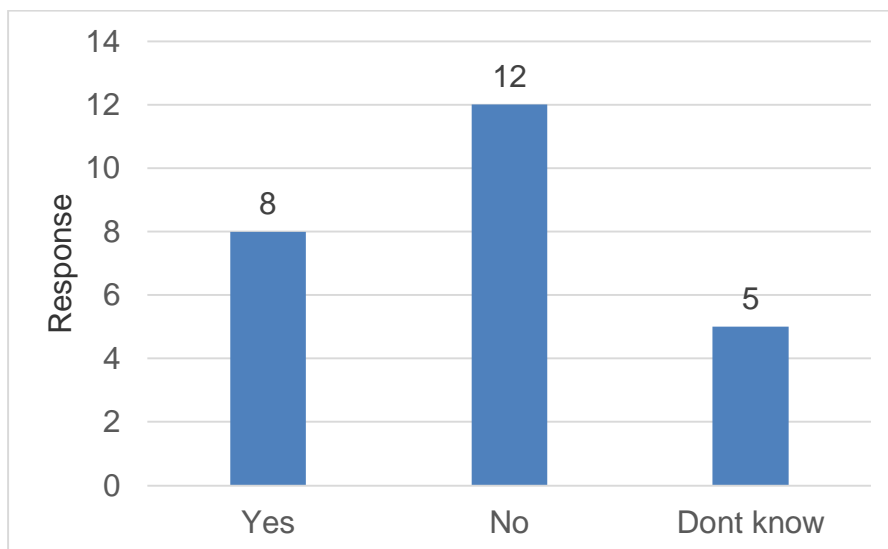
¹ Please note that where graphs do not add up to 26 this is due to not all respondents providing an answer for each question.

Italy	Ukraine
Latvia	Wales
Lithuania	
Luxembourg	

Survey results are reported below across the areas included in the questionnaire: Understanding of the digital environment; National frameworks; National co-operation; Reporting and remedies; International co-operation; and Advice of ENOC Members.

Understanding of the digital environment

1.1 Is there a recognised definition of the digital environment in your jurisdiction?



There was a mixed response from ENOC Members in relation to whether there was a recognised definition of the digital environment in their jurisdiction. Of the 25 Members that responded to this question 12 reported that there was no recognised definition, eight stated that there was and five did not know.

Of those jurisdictions that had a recognised definition in place many respondents cited data protection, cybersecurity or child protection imperatives and few reported that definitions addressed the digital environment in its entirety.

The following are examples of definitions of the digital environment from those respondents that answered yes to this question.

The total of digital resources (computers, software, storage, systems) used to manage an academic enterprise and support, enable or manage learning. (*Cyprus*)

Poland has a national cyber safety strategy 2017-2022.

According to the Law “On the Information, process of informing, protection of information”, information technology is defined as system of methods and ways used during information processes, including application of computing and communication technique (*Azerbaijan*)

The Law of Ukraine “On the Basic Principles of Ensuring Cybersecurity of Ukraine” contains the definition of the cyber space. (*Ukraine*)

Other countries have indicated progress with defining the digital environment:

The Ministry of culture is working on a new definition based on the recommendation of the Council of Europe from July 2018. The Commissioner for Children participates in this process. (*Slovakia*)

1.2 In your jurisdiction is there government or other research on any or all of the following: Children’s use of technology and online safety, child development/child health, mental health, parenting, and children’s views and experiences in their use of digital technology?

The majority of respondents (20 out of 23) reported that government or other research was available on aspects of digital technology, although there was variation in the types of research available. The most commonly cited research related to child protection and child safety online, internet use and devices in the home. A number of countries also referenced research on digital parenting including Estonia, Ireland and the Netherlands.

Some respondents also referred to a broader network of organisations or jurisdictions that provided greater capacity for producing research.

Wales noted that the UK has benefitted from a cross-jurisdictional study, the Millennium Cohort Study, which has been tracking a cohort of children across the UK since they were born in the year 2000. At age 14, they collected data on children’s time use, which included use of technology.

The Safer Internet Centre was referenced by Italy, Latvia and the Netherlands and produces a wide range of research on different aspects of the digital world and

children and young people. The response from Malta noted:

The Office of the Commissioner for Children forms part of the Maltese Safer Internet Centre and therefore makes various remarks and recommendations with regard to children's digital rights.

In Luxembourg there are nationwide training workshops in schools provided by BEE SECURE. The trainers meet thousands of students, parents, teachers, citizens and older people each year and their experiences regarding problems, emerging trends and other observations are regularly recorded and reported.

There was very limited reference to research that considered child health and development and it is notable that most research cited by respondents is quantitative rather qualitative in nature. The limitations of this were highlighted by Norway in their response:

Mostly it is research on limited topics and the ombudsman considers it a problem that we have several topics we need more research on. It is also a problem that there is not much qualitative interdisciplinary research on children and the digital environment.

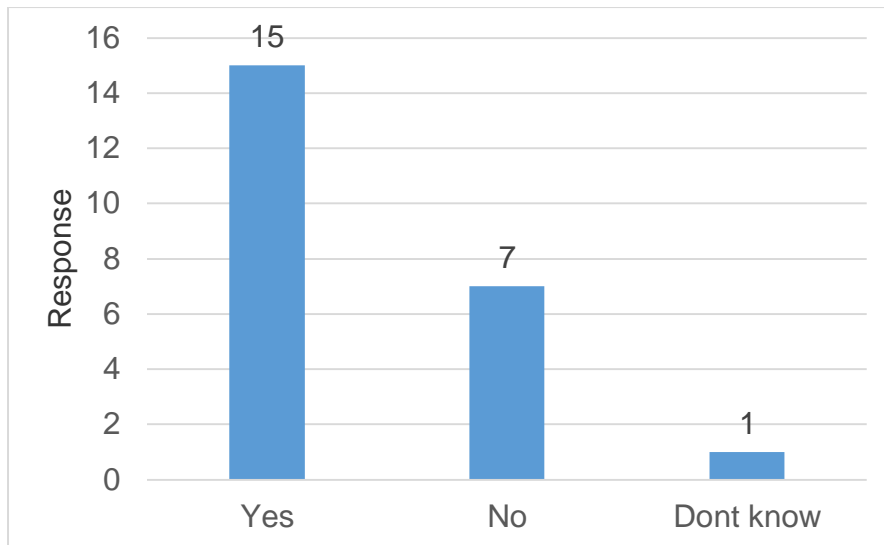
1.3 Has your office undertaken work, published reports and/or made recommendations in relation to the digital environment?

The vast majority of responding ENOC Offices (23 out of 25) had undertaken some work in relation to the digital environment, this included:

- Publishing reports including annual reports, monitoring reports or corporate plans.
- Providing advice to government, responding to national surveys or government consultations.
- Collaborating with organisations working on this area, such as, the National Advisory Council for Online Safety, Safer Internet Centre, Council of Europe and ENOC.

2. National framework within your jurisdiction

2.1 Does your jurisdiction have a legal framework or specific legislation regarding the digital environment?



The majority of respondents (15 out of 23) reported that there was a legal framework or specific legislation in their jurisdiction. A range of legislation was referenced that related to aspects of the digital environment but for most countries there was not an all-encompassing one. Data protection, in particular GDPR, and modernisation of aspects of criminal law was the most commonly cited legislation. Some respondents referred to recent changes in the law or steps to reform legislation to take account of new issues coming to the police and courts, for instance, cyberbullying, sextortion and revenge porn.

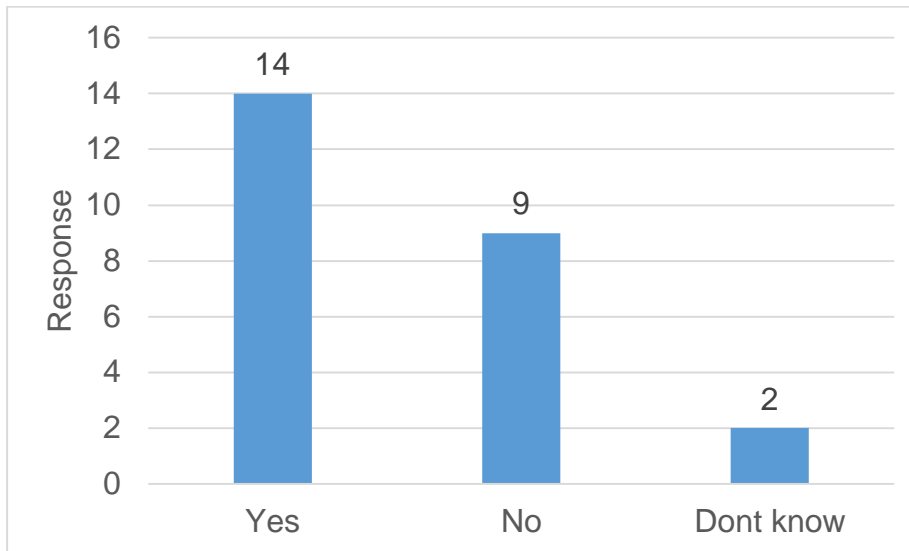
In 2016, the French legal system reinforced existing laws on specific topics (increased fines by the CNIL in case of recurrence, increased sanctions for revenge porn, strengthened obligations for digital businesses regarding transparency and confidentiality), and created new provisions, such as a more protective “right to be forgotten” for children.

In March 2019, the Minister for Communications, Climate Action and Environment in Ireland announced that he is proposing to introduce a new Online Safety Act to improve online safety, including the protection of children online. Among the provisions that it is expected will be made in the Online Safety Act is for the establishment of an Online Safety Commissioner. A public consultation is currently underway.

No-one referred to how commonly used or effective the range of legislation in their jurisdiction was. A number of respondents did make the point that much of the legislation concerning the digital environment was general and not specifically for children and young people.

2.2 Does the legal framework, so far as possible, pursue restorative approaches and prevent criminalisation in relation to online peer to

peer violence and abuse? This may include ‘sexting’ and user generated images.



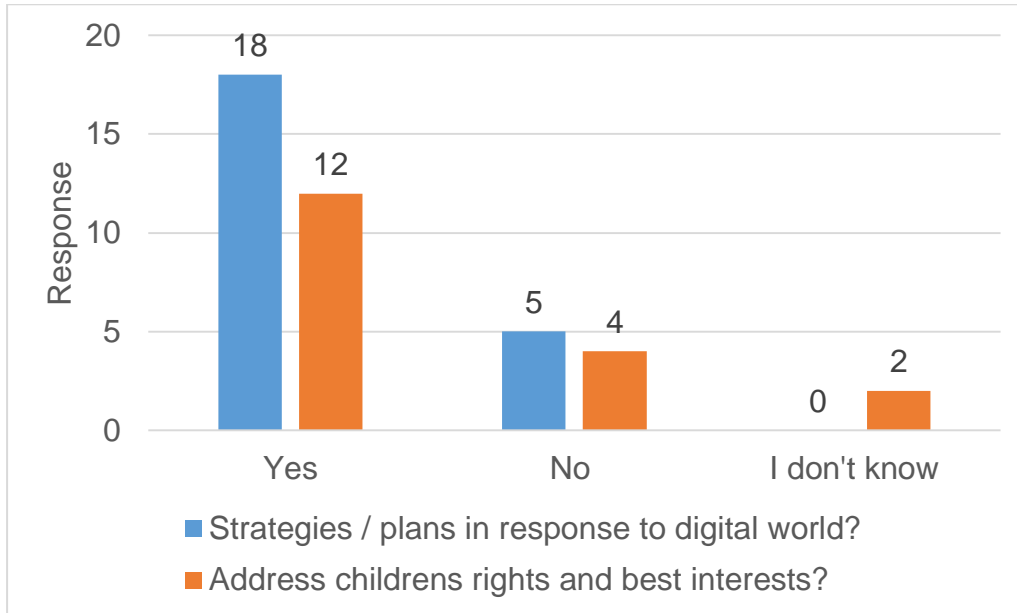
There was a mixed response to the question of whether the legal frameworks across ENOC Members included restorative approaches and prevented criminalisation in relation to peer-to-peer behaviour in this context. Slightly over half of respondents (14 out of 25) indicated that restorative approaches or criminalization prevention were part of their legal framework, however nine indicated that it was not and two did not know.

In Catalan, the approaches to online violence and abuse are similar to the ones provided to similar crimes that can be take place offline. Penal Code has been modified to include some specific crimes on children using internet, telephone and other technologies, but not specifications on restorative and preventing practices. There are programmes to work mainly with children and teenagers on school environments to prevent online abuses and criminalisation (by police and education departments).

In the Netherlands, the attorney general of our Supreme Court advised the government to penalize sexting between teenagers, with the exception of teenagers who are romantically involved with each other. According to the Minister of Justice and security, sexting is normal and acceptable behaviour among modern-day teenagers and should thus not be penalized. Netherlands also has a programme for (potential) young offenders of cybercrime.

In Northern Ireland it was noted that although the legislative framework does not prevent criminalisation due to ‘sexting’, statutory agencies have stated their intention to prevent unnecessary prosecution. However, the Children’s Commissioner has called for further reform.

2.3 & 2.4 Does your jurisdiction have strategies/action plans/policies in place in relation to the digital environment? Do they address children's rights and best interests?



The majority of responses (18 out of 23) indicated that there were strategies, action plans or polices in place in relation to the digital world. However, it was recognised that often reference to these or to actions were fragmented across a range of strategies or plans rather than being part of a single overall strategy, as articulated in the response below:

In France, there is no overall strategy on the subject of the digital environment, but sectoral strategies, such as the 2017 strategy to promote digital inclusion (<https://societenumerique.gouv.fr/strategie-nationale-pour-un-numerique-inclusif/>) Most national strategies, however, have integrated the issue of the digital environment in relation with their specific subject, including strategies focused on children's rights. For instance, the 2017 plan for action violence against children provides measures to prevent the exposure of children to pornography on digital supports.

Of the 18 responses, 12 indicated that they addressed children's rights and best interests.

In Serbia, the Cybercrime Strategy 2019-2023 recognizes fully children's rights and is based on the CRC and other international treaties on children's rights.

In Slovakia, best interests of the child and children's rights is one of the main goals of the upcoming documents.

2.5 Does the national framework include: identification of bodies to implement the strategy/action plan/policies; resources for implementation; engagement of stakeholders including children; and a review of implementation?

In total 17 of 23 responses to this question indicated that a national framework was in place. In some countries, national action plans have a specific focus on children and young people but in others there was not. As already highlighted by respondents, the focus tends to be on specific aspects of the digital environment, most commonly online protection, rather than a more comprehensive plan.

In Italy, the national plan of action states that the Government "shall establish public initiatives to raise awareness on and to prevent online bullying, through the direct involvement of local social and educational services and in cooperation with schools. In the framework of the plan of action ... the Presidency of the Council of Ministers, in cooperation with the Ministry of Education, University and Research and the Authority for Communications shall develop, within the limits of the budget under the first sentence of paragraph 7, regular information campaigns to prevent and raise awareness about cyberbullying, to be published on the main media, the broadcast and printed press and private entities. Starting a year after entry into force of this law, the Minister of Education, University and Research shall submit to Parliament by 31 December each year a report on the outcome of the work of the Board of Experts for the Prevention and Fight Against Online Bullying under paragraph 1 above. For the purposes of enforcing the provisions of paragraph 5, a yearly budget of €50,000 starting in 2017 shall be allocated. This amount shall be made available by reducing the allocation for the years 2017, 2018 and 2019 of the current account special fund 2017-2019 of the "reserve and special funds" of the "available funds" of the Economy and Finance Ministry 2017 budget, partly using the provision of such Ministry. The Economy and Finance Minister may issue orders to make the necessary budget adjustments".

In Ireland, 'Better Outcomes, Brighter Futures' is the Irish Government's national policy framework for children and young people and covers the period 2014-2020. This policy framework makes a number of commitments in relation to children and the digital world. Commitments under Outcome 3 ('Safe and protected from harm') focus on supporting efforts to limit children's exposure to age-inappropriate behaviour online; supporting efforts to combat child sexual abuse, exploitation and trafficking; and promoting best practice by social media providers regarding privacy controls and reporting mechanisms with a view to better protecting children online.

Outcome 5 ('Connected, respected and contributing to their world') includes a commitment to supporting youth organisations to provide quality assured information and support that responds to young people's needs, including online.

2.6 Vulnerable groups: Does this address the circumstances and needs of vulnerable groups, such as, children in care, children in rural areas, children with disabilities, children in detention settings, LGBT+ children?

The majority of responses to this question (13 out of 19) reported that national strategies or action plans did not take account of the circumstances of vulnerable groups of children. In most cases where respondents indicated that a focus was given to children and young people in the national action plan, this tended to be for all children and young people, with no specific reference to or actions for 'vulnerable groups'.

Some responses however, including those from Malta, Montenegro and Poland noted that policies or services did take account of the needs of particular groups of children, such as, children in care, children with disabilities and children in rural areas.

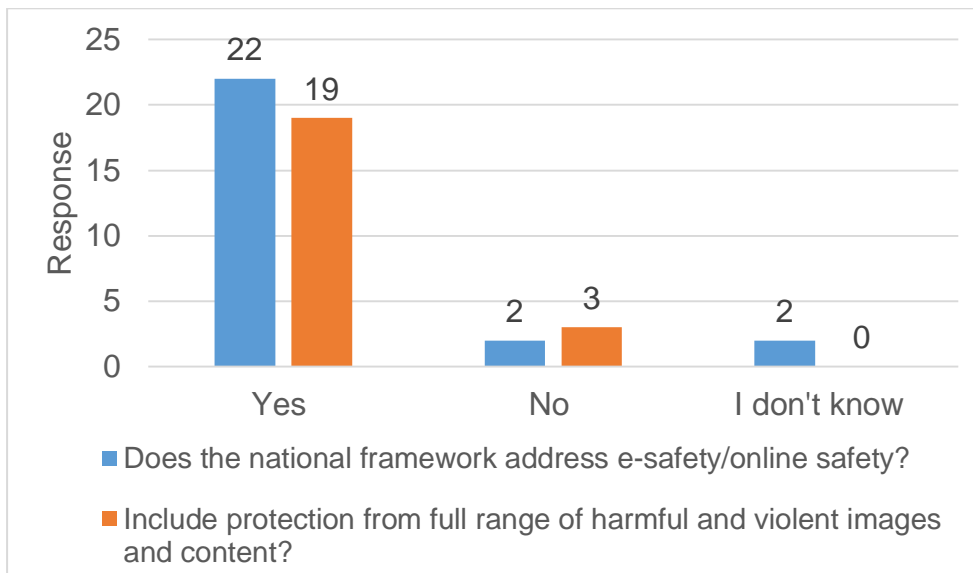
2.7 Participation: Does the national framework address the role of the digital environment in promoting children's participation in local, national and global debates and recognise children as creators and distributors?

Of the 21 responses to this question, over half (n=12) indicated that the national framework does not promote children's participation or recognize their role as creators and distributors of digital material. However, there were eight countries that indicated that this was happening while one did not know.

In Cyprus, under the National Strategy, the CYbersafety Youth Panel has been established, with members of the Cyprus Youth Parliament, the Cyprus European Youth Parliament, Commissioner's Young Advisors. The CYberSafety Youth Panel allows young people to express their views and exchange knowledge and experiences concerning their use of digital and online technologies, as well as tips on how to stay safe. They also advise on the strategy for the creative use of digital and online technologies with safety and responsibility, help create innovative resources and disseminate eSafety messages to their peers and other audiences.

In Montenegro, promoting children’s participation in policy is mainly only evidenced by the Childrens Ombudsperson and UNICEF. The Ombudsperson has direct and continuous communication with children through regular activities and direct work with children and through the Golden Advisers’ Network, which is a permanent body of the Ombudsperson and consists of 25 children of different ages from different towns of Montenegro. These children actively participate in all activities of the Ombudsperson as well as in the preparation of documents, advertising materials, research, analyses and recommendations.

2.8.1 & 2.8.2 Protection: Does the national framework address e-safety/online safety? Does this include protection from the full range of harmful and violent images and content (including child sex abuse; grooming; adult content; bullying; harassment; self-harm and suicide; radicalisation; racism and hate speech and commercial exploitation)?



The vast majority of respondents (22 out of 26) indicated that their national framework addresses online or e-safety safety. However, a number of ENOC Members, including Estonia, highlighted that digital protections are addressed across a range of laws or strategies.

Estonia reported that the elements listed above are addressed in different laws. Child Protection Act prohibits dissemination of objects (printed matter, films, audio and video recordings and other objects) with pornographic content and promoting violence. Penal Code stipulates punishments for: requesting access to child pornography and watching thereof; manufacture of works involving child

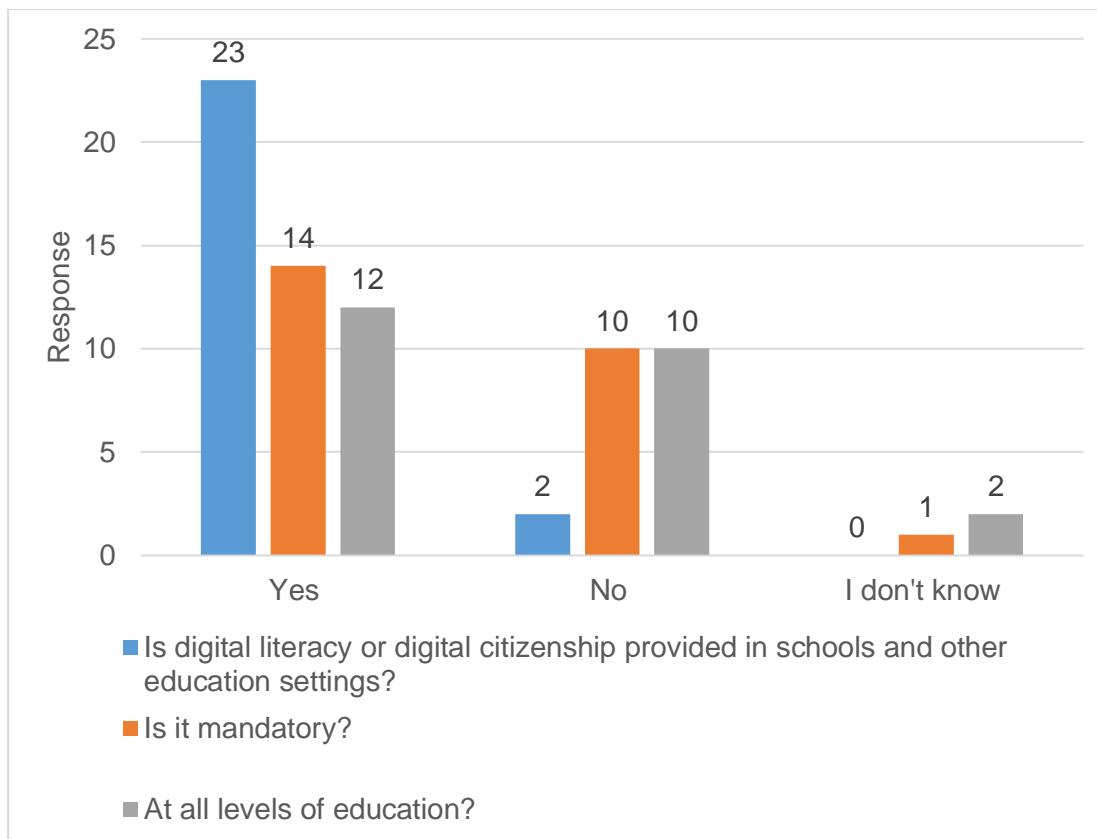
pornography or making child pornography available; agreement of sexual purpose for meeting with child; sexual enticement of children; exhibiting cruelty to minors.

Most also indicated that national frameworks included protection from a wide range of harmful and violent images and content (19 out of 22). However, a number of respondents noted that there may still be gaps in protections, for example, Cyprus indicated that current provisions do not fully take account of the risks young people face online from grooming and radicalization. Other respondents gave examples of protection measures being available in specified circumstances:

In Finnish law sexual harassment and exploitation in digital environment are not specially criminalised but may fall in scope of criminal code crimes such as sexual exploitation, possessing and sharing pictures of children that are against the sexual morality or grooming (often in social media), that was criminalized in 2011.

In Montenegro, the Agency for Electronic Media has recently banned inappropriate contents on the national frequencies – television media by protecting certain contents with a PIN code and the parents then have the responsibility to decide whether the child will be allowed to watch the inappropriate contents.

2.9.1- 2.9.3 Education: Is digital literacy or digital citizenship provided in schools and other education settings? Is it mandatory and in all levels of education?



The vast majority of respondents (23 out of 25) stated that digital literacy or citizenship was provided in schools or other educational settings. However, as indicated in the graph above, there was a more mixed picture in relation to whether digital literacy or citizenship was mandatory and whether it was provided at all levels of education.

Some respondents cited that guidance was available for teachers in their country on content:

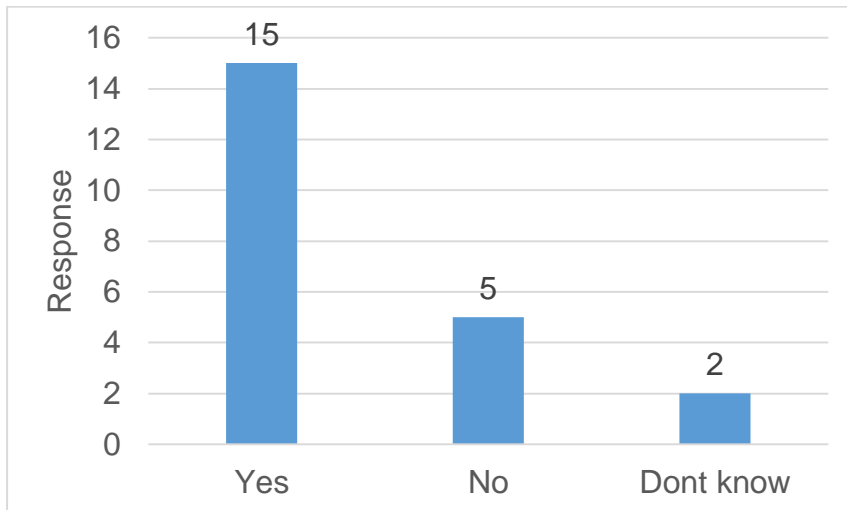
In Wales, the Digital Competence Framework is part of the new school curriculum, which will be used throughout Wales by 2022. Digital competence is a cross-curricular responsibility alongside literacy and numeracy. The Digital Competence Framework guidance for teachers is separated into four strands: Citizenship, Interacting and collaborating, Producing and Data and computational thinking. Citizenship includes identity, image and reputation, health and well-being, digital rights, licensing and ownership, online behaviour and cyberbullying.

In the Basque region, digital skills are provided at all levels of education (from pre-school to university) as basic cross-cutting skills in line with the European Parliament and Council Recommendation of 18 December 2006, on keys competences for life-long-learning (2006/962/CE).

Some Members, such as Northern Ireland, raised specific concerns regarding the

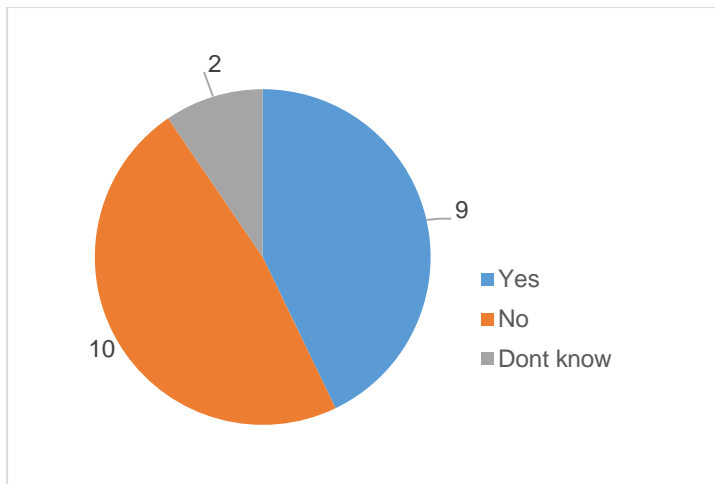
lack of a mandatory curriculum to ensure that high quality digital literacy or citizenship was provided in all education settings.

2.10 Data: Does the national framework address processing and protecting children’s data, including privacy by design; restrictions on the use of sensitive data; age verification and ensuring children/parents and carers/legal representatives provide informed consent?



The majority of respondents (15 out of 22) reported that there was data protection legislation their country and GDPR and DPA were commonly referenced. However, a number of jurisdictions noted that legislation and its implementation may address some but not all of the relevant issues regarding the processing and protection of children’s data. Some respondents, including Catalan and Norway, also raised concerns that even when legislation is in place enforcement can be weak.

2.11 Does your jurisdiction provide government or official guidance on children’s use of social media and/or screen time?



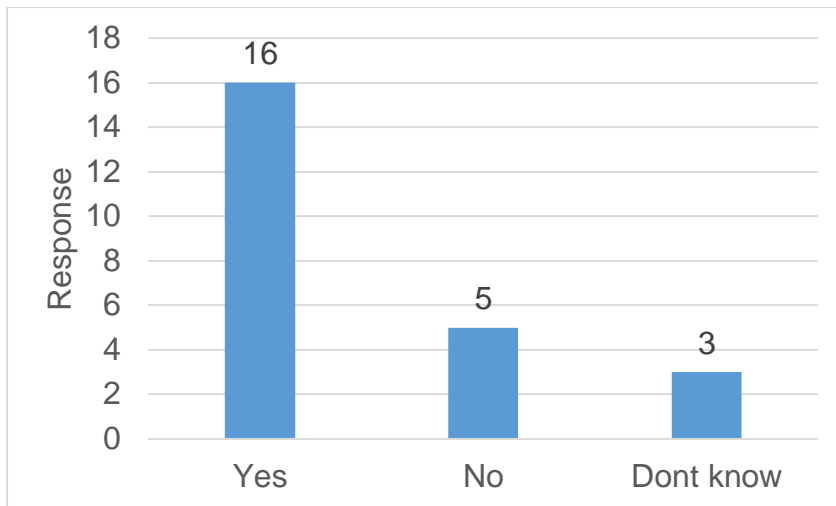
There was a mixed response to the question about whether official guidance on safe use of social media or screen time for children was available with, essentially, an equal proportion of countries reporting 'yes' (n=9) and 'no' (n=10).

Some of the responses also highlighted an ongoing debate around this issue, illustrated by Norway:

There is some advice given by governmental agencies for parents on the use of social media. Little on screen time. There is a need for more information on children's use of social media. In Norway this has mostly been a debate on age limits. There has also been a big debate on the ban of cellphones in schools. The Ministry of Education is clear that the use of phones in schools must be decided by the municipalities or schools.

3. National co-operation within your jurisdiction

3.1 Is there a framework or mechanism for co-operation between government authorities, independent authorities, civil society and business enterprises?



The majority of the respondents reported that a framework or mechanism for co-operation was in place (16 out of 24). However, there was some variation in the structure and membership of mechanisms:

In Albania, the government is establishing an Advisory Technical Committee on Child Safety on the Internet, at the National Council for the Rights and Protection of Children. It is proposed that the committee, consisting of one representative from each signatory ministry, one member from AMSHDF, State Police, AKCESK, AKEP etc. A member of the committee may be any organization of civil society, public institution, Telecommunications Company etc. The modalities of the establishment and functioning of the committee are defined by the instruction of the minister responsible for children in Albania

In Cyprus, the National Strategy for a Better Internet for Children includes a network called CYberSafety, which brings together major national stakeholders in order to create a safe internet culture, empowering creative, innovative and critical citizens in the digital society. CYberSafety aims to provide an awareness platform where actors can find resources and tools, share experiences, expertise and good practices. At the same time it aims to contribute towards a European approach and provide qualitative and quantitative feedback at European level, through the core service platform.

In France, the CNIL (National Commission on Informatics and Liberty) is an independent French administrative regulatory body in charge of ensuring the application of data privacy law. It produces guidance and initiatives about children's rights in a digital environment, with the "Educnum" group. With its counterpart authorities, the CNIL agreed on an international standard on digital education. "Eudacdroit", a project created by the Defender of Rights, creates tools to educate children to their rights. Eudacdroit has created a working group on "law and the digital environment", in cooperation with the CNIL.

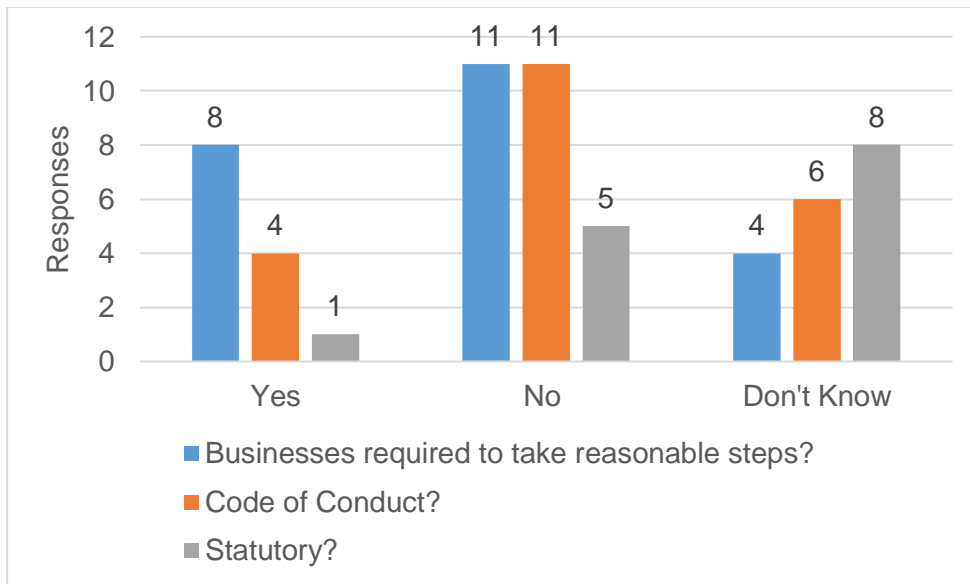
The CSA (Superior Council of the Audiovisual, an independent regulatory institution) integrated the issue of the digital environments in the works of its expert committee on the protection of young public.

The French government's "inter-ministerial action plan for mobilizing and combatting child abuse" contains provisions to prevent the exposure of children to pornography on digital media.

In Luxembourg, Digital Luxembourg is a multi-disciplinary governmental initiative collaborating with public, private and academic stakeholders to exploit digitalisation and to achieve a positive digital transformation. In order to achieve this goal, digitalisation is tackling globally, focusing on the strengthening and the future of five priorities: skills, policy, infrastructure, ecosystem and government. By executing the digitalization strategy of the Luxembourg government, Digital Luxembourg is launching new projects, supporting existing ones and boosting the visibility of national efforts.

In Malta as part of the Safer Internet Centre there is an Advisory board which brings together key stakeholders which inform the work carried out by the safer internet centre. The safer Internet Centre also coordinates 3 different fora which also feed into the advisory board, namely, the parent/carer forum, the psycho-social forum and the industry forum.

3.2-3.3.2 Are businesses and others required to take reasonable steps to ensure they undertake child rights impact assessments; that their terms and conditions are enforced; that requirements are in place regarding safety and privacy by design; age verification; and that child protection policies and vetting procedures? Is there a code of conduct for digital business? Is it statutory?



In relation to business practices and standards regarding the digital environment, the survey responses highlight a mixed picture in relation to measures, such as obligations on business, being known to be in place. A number of respondents were unsure about practices and statutory arrangements in their jurisdiction, perhaps indicating wider issues about the need for more progress, awareness and transparency in this area.

Serbia reported that apart from legal provisions regarding criminal acts and children in media and advertising, there are no other legal provisions, which would put additional requirements on companies.

In Latvia, there are no general codes of conducts in our jurisdiction, but a lot of companies have their own codes of conduct.

Denmark was the only country that referred to having a statutory code for digital businesses in their country.

Most respondents indicated that where an industry code of conduct was in place these tended to be self-regulated. In some areas, such as the UK, there is currently a lively debate and ongoing developments, regarding statutory regulation for industry.

4. Reporting and remedies

4.1 - 4.6 Do children, their parents/carers or legal representatives have access to reporting mechanisms (including for the reporting of child

abuse material)?

	Yes	No	Don't Know
Access to reporting mechanisms?	25	0	0
Reports made anonymously?	21	2	1
Children or Parents/ Carers have access to support?	23	0	1
Access to legal remedies?	20	1	3
A range of legal remedies available?	19	1	4
Child Friendly material on reporting and remedies?	15	5	3

As shown in the table above, all respondents to the question stated there was some form of access to reporting mechanisms in their jurisdiction. While the majority of responses noted that they had the facility to make reports anonymously, two stated that this was not the case.

Belgium (Flemish Region) raised the point that although mechanisms for remedy were available in their country, they 'are not very accessible and effective in practice.'

Estonia has web-constables who provide advice about internet safety and if necessary forward information or proceeding to relevant police stations. Web-constables are police officers working in internet. They respond to notifications and letters submitted by people via internet and train children as well as adults at issues of internet security. They also help to remove unlawful content. For compensation one has to go to court.

Save the Children Finland hosts a web page where anyone can give information about illegal activity concerning sexual exploitation of children. It is also possible to contact police about that kind of material. In 2019 a new web page Someturva (www.someturva.fi) gives expert guidance to bullying, harassment and threats in social media (some). The service is youth and child friendly. The page is run by Save the Children Finland, Ministry of Justice and Ministry of the Interior.

The vast majority of respondents also reported that there was support available for children and parents or carers. Most referenced this support being available via generic services rather than specialised support in relation to the digital environment and online safety. However, Denmark and Luxemburg did cite specialised helplines regarding digital media.

5. International co-operation

5.1 Has your jurisdiction ratified the following instruments?

The table below shows that most countries have ratified each of the international instruments listed. However, it is of note that this is not the case in all instances, particularly in relation to the UNCRC Optional Protocol on a communications procedure and the Council of Europe Convention on Cybercrime.

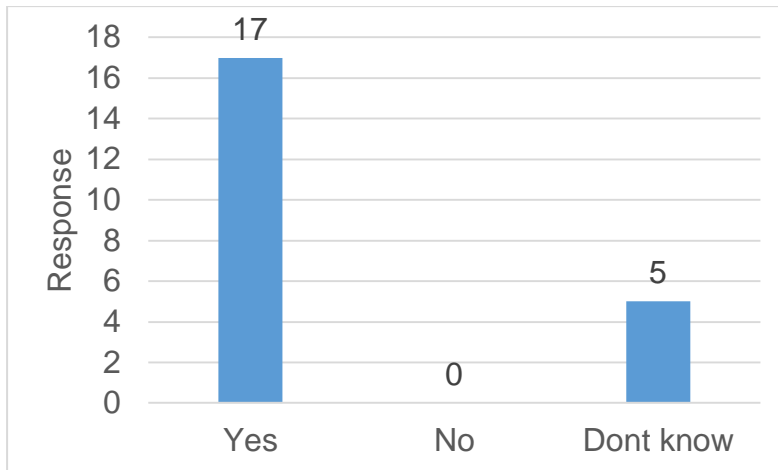
	Yes	No	Don't know
Optional Protocol to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000);	23	1	0
Optional Protocol to the United Nations Convention on the Rights of the Child on a communications procedure (2011);	14	10	0
Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);	22	0	2
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);	18	5	1
Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197);	22	1	1
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).	22	2	0

5.2 Is there an adequate legal basis/treaties/other mechanisms to ensure international co-operation, including making and executing requests for assistance and information?

There was a relatively low response to this question (n=18) with only 11 respondents agreeing that there was an adequate legal basis or mechanisms for ensuring international co-operation and eight indicating that they did not know.

Northern Ireland raised specific concerns about the impact of Brexit and the lack of certainty about future co-operation with European bodies (such as Eurojust) and mechanisms (such as the European Arrest Warrant).

5.3 Can criminal justice agencies connect with INTERPOL in relation to child sex abuse material and ICANN in relation to identifying and removing web addresses which promote child sex abuse or other child abuse material?



The majority of respondents (17 out of 22) reported that their jurisdiction could connect with INTERPOL and ICANN. No respondents indicated that this was not the case while five stated they did not know.

6. Advice of ENOC offices

6.1 Are there examples of best practice from your jurisdiction, such as, children's involvement in policy development, production of accessible terms and conditions, child friendly reporting mechanisms?

Examples of existing practice reported by ENOC Members are provided throughout the report, however in response to this question 18 of the 26 Members provided specific examples.

In Estonia, a youth panel convened as part of the Smartly on the Web project advise the project team on the planning and implementation of activities aimed at young people. The panel passes on young people's views regarding the kind of information they need to use the Internet safely and successfully and how this information would best be conveyed to kids.

Lithuania stated that they had a very successful project initiated by the private telecommunication company "Telia" <https://auguinternete.lt/>. They also referred to

their child friendly reporting mechanisms, and how policy and good practices inform the scope of the Safer internet project in their country which includes a youth forum.

In Montenegro, the Protector of Human Rights and Freedoms – Ombudsperson has a “Brave Mailbox” on its website intended for reporting abuse on the Internet – intended for children. The Protector’s Brave Mailbox is directly linked to the CIRT program. The golden box as a mechanism for reporting inappropriate content that is available to children on the Internet and abuse of children on the Internet is, in addition to the Ombudsperson’s website, also promoted on current social networks.

The response from Bosnia-Herzegovina also notes that children and parents can report any form of violence through anonymously through a "courageous mailbox".

Serbia highlighted that there had been a national campaign on prevention from cyber predators on social networks through short videos published on TV channels with national frequency, other TV channels, internet (ads on popular content on the internet), etc. The only deficiency of this campaign was that it was too short as it lasted only couple of months.

6.2 What are the priority areas for the work of your office in relation to ensuring children’s rights in the digital environment?

The majority of ENOC Members (n= 22) highlighted priority areas of work for their offices in relation to children’s rights in the digital environment. This included: awareness raising of the dangers of online world; highlighting a child rights basis for the digital environment; the impact of screen time on young children; stressing the need for national mechanisms to strengthen regulation on all aspects of internet safety; the need for further inter-disciplinary research and cross-sectoral training and informing the drafting of Government e-safety strategy or action plans. Four respondents were not planning any further work.

6.3 What are the three priority issues which your office advises should be addressed in ENOC’s statement on children’s rights in the digital environment?

Twenty of the responding jurisdictions provided advice on issues that should be addressed in the ENOC Statement on children’s rights in the digital environment.

The following provides a summary of some of the main priorities identified:

- Addressing new and emerging issues, such as, the impact on children’s health and development (including toxic technology), on parenting and persuasive design.

- Advocating for the introduction of statutory codes of conduct and regulation of industry, addressing for instance, accessible terms and conditions, informed consent and safety and privacy by design.
- Awareness raising with children and parents / carers of the dangers in the digital environment, including reporting mechanisms and protections after reporting.
- Protection of children from harmful information and content.
- Violence or harassment against children, including peer-to-peer.
- The right to universal access: adequate, accessible and secure access.
- Fake news and disinformation on the internet.
- Supporting practical implementation of the Council of Europe Recommendation.
- Mobilising general measures for implementing children's rights under the UNCRC

The response from the Basque Country stated that although it is not specifically focused on children and young people, the Universidad de Deusto recently presented an "On-line Declaration of Human Rights" which could be a useful reference document for the ENOC statement and recommendations.

6.4 In completing this questionnaire has your office engaged with children and young people and/or drawn on research or evidence which involved children and young people.

Of the 20 responses to this question, 11 indicated that they had engaged with children and young people or drawn on research / evidence which involved children in completing the survey and eight had not. A number of countries, including Albania, Estonia and Serbia consulted with young people via workshops or focus groups to inform the completion of the questionnaire and a number of the other ENOC Members stated that they were planning to start engagement as part of the ENYA (European Network of Youth Advisors) Project on children's rights in the digital environment.



This publication was co-funded by the European Union's Rights, Equality and Citizenship Programme (REC 2014-2020). The content of this publication represents only the views of ENOC and is its sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Appendix One: ENOC Questionnaire

ENOC Members Questionnaire: Children's rights in the digital environment

Introduction

In 2019 the theme of ENOC's statement has been agreed as children's rights in the digital environment. The purpose of ENOC's annual statement is to make recommendations which will improve the fundamental rights of children and young people with regard to the United Nations Convention on the Rights of the Child and its founding principles.

As the draft statement is developed it is important to ensure that:

- the statement reflects the views and experiences of ENOC members; and
- the recommendations take account of the range of protections and positive measures that are in place across our jurisdictions as well as drawing attention to improvements that are needed to promote and safeguard children's rights.

We are aware of the parallel participation project that many ENOC members are taking part in through ENYA and hope that throughout the development of the statement, including in the completion of this questionnaire, members are able to incorporate the views of children and young people in their comments.

We hope that you are able to take part in this survey and can return information by **Thursday 21 March 2019**. We welcome all contributions and appreciate that members may only be able to complete some sections of the questionnaire.

Please note that we may produce a summary paper as part of the drafting process and may include feedback and information from the questionnaire in this.

Background

The digital environment offers a wide range of positive opportunities for children and young people to further realise their rights under the United Nations Convention on the Rights of the Child. This ranges from contact with distant family members and friends, accessing material for learning and education, seeking and receiving information and support, being able to participate in myriad ways and to create and distribute material.

However, ENOC's decision to develop a statement on children's rights in the digital world is timely as concerns about our lack of understanding about the impact of digital technology on children's development, safety and well-being as well as on parenting and family life is growing alongside concerns about the collection, tracking and use of children's data through connected technologies and a range of other applications.

In July 2018 the Council of Europe issued a comprehensive recommendation to the Committee of Ministers to member States [MC/Rec\(2018\)7](#) addressing many of these issues and the United Nations Committee is developing a General Comment on children's rights in the digital world. The 2019 ENOC statement provides an important opportunity to bring attention to the need to understand children's rights in the context of our rapidly changing digital environment and to ensure that governments and others across voluntary and private sectors are taking all necessary steps to promote and safeguard children's rights and to ensure their participation in this regard.

Please note:

The term 'child' or 'children and young people' is used to indicate those under the age of 18 years.

The term 'digital environment' refers to information and communication technologies (ICTs) including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services as set out in MC/Rec(2018)7.

Name of Office:

Contact name:

Contact details:

1. Understanding of the digital environment

1.1 Is there a recognised definition of the digital environment in your jurisdiction?

Yes Don't know No

Please provide details:

1.2 In your jurisdiction is there government or other research on any or all of the following:

Children's use of technology; online safety; digital technology and child development/child health; digital technology and mental health; parenting and digital technology; children's views and experiences in their use of digital technology?

Yes Don't know No

Please provide details of or links to research:

1.3 Has your office undertaken work; published reports and/or made

recommendations in relation to the digital environment?

Yes No
Don't know

Please provide details:

2. National framework within your jurisdiction

2.1 Does your jurisdiction have a legal framework or specific legislation regarding the digital environment?

Yes No
Don't know

Please provide details:

2.2 Does the legal framework, so far as possible, pursue restorative approaches and prevent criminalisation in relation to online peer to peer violence and abuse? This may include 'sexting' and user generated images.

Yes No
Don't know

Comments:

2.3 Does your jurisdiction have strategies/action plans/policies in place in relation to the digital world?

Yes No
Don't know

2.4 Do these address children's rights and best interests?

Yes No
Don't know

Please provide details:

2.5 Does the national framework include: identification of bodies to implement the strategy/action plan/policies; resources for implementation; engagement of stakeholders including children; a review of implementation?

Yes No
Don't know

Comments:

2.6 Vulnerable groups: Does this address the circumstances and needs of vulnerable groups, such as, children in care, children in rural areas, children with disabilities, children in detention settings, LGBT+ children?

Yes No
Don't know

Comments (Please specify any other vulnerable groups):

2.7 Participation: Does the national framework address the role of the digital environment in promoting children’s participation in local, national and global debates and recognise children as creators and distributors of content?

Yes No
Don't know

Comments:

2.8 Protection: Does the national framework address e-safety/online safety?

Yes No
Don't know

Does this include protection from the full range of harmful and violent images and content (including child sex abuse; grooming; adult content; bullying; harassment; self-harm and suicide; radicalisation; racism and hate speech and commercial exploitation)?

Yes No
Don't know

Comments:

2.9 Education: Is digital literacy or digital citizenship provided in schools and other education settings?

Yes No
Don't know

Is this mandatory?

Yes No
Don't know

Is this provided at all levels of education?

Yes No
Don't know

Comments:

2.10 Data: Does the national framework address processing and protecting children's data, including promoting privacy by design; restrictions on the use of sensitive data; age verification and ensuring children/parents and carers/legal representatives provide informed consent?

Yes No
Don't know

Comments:

2.11 Does your jurisdiction provide government or official guidance on children's use of social media and/or screen time?

Yes No
Don't know

Please provide details:

3 National co-operation within your jurisdiction

3.1 Is there a framework or mechanism for co-operation between government authorities, independent authorities, civil society and business enterprises?

Yes No
 Don't know

Comments:

3.2 Are businesses and others required to take reasonable steps to ensure they undertake child rights impact assessments; that their terms and conditions are enforced; that requirements are in place regarding safety and privacy by design; age verification; and that child protection policies and vetting procedures?

Yes No
 Don't know

Comments:

3.3 Does your jurisdiction have a code of conduct or similar arrangement for digital businesses?

Yes No
Don't know

Is this statutory?

Yes No
Don't know

Please provide details:

4 Reporting and remedies

4.1 Do children, their parents/carers or legal representatives have access to reporting mechanisms (including for the reporting of child abuse material)?

Yes No
Don't know

4.2 Can reports be made anonymously?

Yes No
Don't know

Comments:

4.3 Do children and parents/carers have access to support services, helplines and counselling?

Yes No
Don't know

Comments:

4.4 Do children, their parents/carers or legal representatives have access to remedies?

Yes No
Don't know

4.5 Does this include rights to correction; removal of unlawful content; apologies; compensation (including from perpetrators)?

Yes No
Don't know

Comments:

4.6 Is child friendly information provided on reporting and remedies?

Yes No
Don't know

Comments:

5 International co-operation

5.1 Has your jurisdiction ratified the following instruments?

Optional Protocol to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000);

Yes No
Don't know

Optional Protocol to the United Nations Convention on the Rights of the Child, and on a communications procedure (2011);

Yes No
Don't know

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);

Yes No
Don't know

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);

Yes No
Don't know

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

Yes No
Don't know

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

Yes No
Don't know

5.2 Is there an adequate legal basis/treaties/other mechanisms to ensure international co-operation, including making and executing requests for assistance and information?

Yes Don't know No

Comments:

5.3 Can criminal justice agencies connect with INTERPOL in relation to child sex abuse material and ICANN in relation to identifying and removing web addresses which promote child sex abuse or other child abuse material?

Yes Don't know No

Comments:

6 Advice of ENOC offices

6.1 Are there examples of best practice from your jurisdiction, such as, children's involvement in policy development, production of accessible terms and conditions, child friendly reporting mechanisms?

Please provide details:

6.2 What are the priority areas for the work of your office in relation to ensuring children's rights in the digital environment?

Please provide details:

6.3 What are the three priority issues which your office advises should be addressed in ENOC's statement on children's rights in the digital environment?

Please provide details:

6.4 In completing this questionnaire has your office engaged with children and young people and/or drawn on research or evidence which involved children and young people.

Yes

No

Don't know

Comments:

Any other comments:

Thank you for your time in completing this questionnaire.

If you have any questions about the survey please contact Jacqueline Melville:
jacqueline@niccy.org