2020

CHILD ONLINE SAFETY IN SCHOOLS

POLICIES AND PRACTICES IN EDUCATION

International Centre “La Strada Moldova”

Public Association
International Centre "La Strada Moldova"

Child online safety in schools. Policies and practices in Education.

Author:

Elena BOTEZATU, lawyer, director of Issues Affecting Children Program at "La Strada Moldova"

Contributions:

Cristina VAȘCHEVICI, educational psychologist
Victoria GRIBINEȚ, psychologist

Research coordinator:

Ana REVENCO

For additional information regarding the present publication, you can contact us at:

MD-2012, CP 259, Chisinau, Republic of Moldova

Tel.: +373 22 23 49 06
Fax.: +373 22 23 49 07
E-mail: office@lastrada.md
Web: www.lastrada.md

Contents

Introduction

We live in unprecedented times where technologies influence our lifestyle, relationships, field of work, and any type of social interaction. In this concoction of changes, children are, perhaps, the most active consumers of information technologies, and also the most vulnerable to online risks, due to their age and lack of knowledge and skills. Trends show that children use the Internet and technologies from a young age, and without the proper support and guidance from their family, educators, community, they could expose themselves to a large spectrum of risks harmful to their emotional wellbeing.

The national context, however, indicates a low level of information in parents, of training in teachers and of community awareness in general to be able to face these changes. There are some backlogs in the adaptation of the process and the contents of education to the current needs of children, in line with global trends. At present, the educational process is oriented towards sporadically organized activities or lessons about the correct use of digital devices, and some rules for online conduct. Moreover, there is a lack of intervention procedures for situations of online abuse, and when such situations happen, actions are taken intuitively.

In order to deal with these changes and cultivate safe online behaviours in children, to raise their level of resilience towards online violence, on the European level, a comprehensive approach to online safety in schools is promoted, which involves all the actors of the educational system. What does this complex approach to online safety mean? What are the challenges and needs of the actors in the field of Education from the Republic of Moldova regarding child online safety? How can the response of the educational system be improved in this regard? These are the key-questions that we are aiming to answer through this research, in order to ensure a better understanding of *online safety in the context of education, of the comprehensive approach model to online safety in schools* and of the necessary conditions for the implementation of such model in the Republic of Moldova.

Methodology

This research intends to analyse the response of the educational system in promoting child online safety through researching the policies and practices of the educational institutions that aim to contribute to the prevention of online risks and protection of children from online abuses.

Objectives:

1. To study the international and national recommendations' framework regarding child online safety in the context of Education;
2. To identify, on a national level, the issues regarding child online safety that need to be solved through educational measures;
3. To elaborate recommendations for improving the response of the educational system in promoting child online safety.

Research tasks:

1. To study policies, recommendations and international commitments undertaken by the RM regarding online safety in the educational process;
2. To study the European comprehensive approach model to child online safety in schools and the good practices of implementation of this model;
3. To analyse the interests and risks that children are exposed to online;
4. To analyse the level of information and preparation of students, teachers and parents in observing and responding to these risks;
5. To analyse the educational measures promoting online safety planned in national policy documents;
6. To analyse the national normative framework in regard to child online safety and to establish the shortcomings that impede the efficient response of the educational system;
7. To study institutional policies and the method of coordination of efforts in the field of online safety in schools; to study the availability of training activities for teachers, intervention procedures in case of an online abuse, partnerships and collaboration with parents in promoting online safety; to study educational methods on the topic of online safety, the main aspects covered and the practices used to secure the ICT infrastructure in schools;
8. To formulate public policy proposals to remediate identified shortcomings and gaps in the national educational practices to ensure the necessary conditions for the implementation of the comprehensive education approach model to online safety in schools.

Research methodologies:

To achieve the objectives of this research, the following tools and methodologies were used:

1. Analysis of international policies and recommendations on how to approach online safety in the educational process;
2. Analysis of policy documents and normative documents of the RM, relevant to the goal of this research;
3. Focus-group discussions with 50 teachers from 48 educational institutions from 20 country districts and Chisinau;
4. Focus-group discussions with school management representatives from 5 educational institutions from 4 towns/villages;
5. Focus-group discussions with 203 secondary school students: 104 from the 6th grade and 99 from the 9th grade;
6. Observation method during the activities on online safety carried out for 69 school psychologists and specialists from the Psycho-pedagogical Assistance Service;
7. Questionnaire on child online safety (completed by 153 parents).

Limitations

The research area of this study is limited to the main issues related to child safety in the online environment and does not address topics such as digital or cyber security. The following topics will not be also covered in this research:

- Digitalisation of the educational system and the use of technology in the educational process;
- Analysis of the digital competencies of teachers, students or other actors in the field;
- Ways in which social networks are used by employees of educational institutions;
- Safety and security of the remote educational process;
- Other aspects related to the integration of ICT into Education, unless they are directly related to online risks that children are exposed to, according to chapter II.

1. International recommendations' framework

1.1. International policies and commitments

For several years, the international community has been concerned with child online safety and the way in which schools can develop critical thinking skills in students so that they can deal with online risks. Educational measures have been established in a number of policy documents and international recommendations, which will be referred to in this research.

General policy framework and international commitments of the RM

The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)[1]

The Republic of Moldova ratified the Lanzarote Convention in 2012 and committed to its implementation[2]. Although the Convention establishes measures of protection of children from all forms of sexual abuse and exploitation, art. 6 provides educational measures that need to be taken to ensure that all children are informed about the risks of sexual abuse and they ways through which they can defend themselves, depending on their level of development. The Convention establishes that special importance must be paid to risky situations involving the use of new information and communication technologies.

Protecting children from sexual exploitation and sexual abuse facilitated by information and communication technologies is the subject of the second round of monitoring the implementation of the Lanzarote Convention, initiated in 2017[3]. Although the monitoring report has not been published yet, data from the monitoring questionnaire includes multiple questions related to the educational system and the measures taken to prevent the transmission of intimate self-generated photographs or videos, which indicates the aspects that need to be approached in the school program to prevent the risks of online sexual abuse[4].

Sustainable development goals

The safety of children online in educational institutions contributes directly to the achievement of the Sustainable Development Goal (hereinafter SDG) no. 4, "Quality Education", and SDG 16, Target 16.2, "Stopping Abuse, Neglect, Exploitation, Trafficking and All Forms of Violence and Torture of Children"[5].

SDG no. 4 "Quality Education"

In Moldova, Goal 4 envisages achieving universal and inclusive education, but also preparing the youth and adults to better fit the labour market. The targets are: sustainable development and sustainable lifestyles, human rights, gender equality, a green economy, promotion of a culture of peace and non-violence, global citizenship and appreciation of cultural diversity, all promoted through their integration in the educational curricula (Target 4.7). One of the challenges to be also addressed relates to ensuring education facilities that are child-, disability- and gender-sensitive, and providing a safe, non-violent, inclusive and effective learning environment for all (Target 4.a).

Safety in the educational institution involves creating an environment where the child feels physically, emotionally and socially safe. A friendly and safe school environment involves an environment that ensures the wellbeing of children, respects their rights and guarantees protection of their physical and psychological integrity. In the context of the digitalization of social relationships, particularly by students, the commitments made by educational institutions to create a safe environment should include the online environment as well as the offline environment.

SDG no. 16 "Peace, Justice and Strong Institutions"

This Goal from the 2030 Agenda in Moldova aims to develop effective, accountable and transparent institutions at all levels, which will ensure a responsive, inclusive, participatory and representative decision-making process on public policy

1 *https://rm.coe.int/1680084822*

2 *https://www.legis.md/cautare/getResults?doc_id=13045&lang=ro (RO)*

3 *https://rm.coe.int/thematic-questionnaire-for-the-2nd-monitoring-round-on-the-protection-/168075f307*

4 *https://rm.coe.int/thematic-questionnaire-for-the-2nd-monitoring-round-on-the-protection-/168075f307*

5 *https://www.md.undp.org/content/moldova/en/home/sustainable-development-goals/goal-16-peace-justice-and-strong-institutions.html*

development and use of public money. An important focus will be placed on the reduction of all forms of violence, especially domestic violence and sexual violence, and ending and combating abuse, trafficking and violence against children (Target 16.2).

Abuse and violence against children can be manifested in schools, where they should be protected and cared for, at home or in the online environment. "Moldova 2030" is an opportunity to elaborate policies that would protect children from all forms of violence, including online violence.

Thematic policy framework regarding the online safety of children during the educational process

The European Strategy for a better internet for children[6]

The strategy is based on four main pillars: 1) Stimulating quality content online for young people; 2) Stepping up awareness and empowerment; 3) Creating a safe environment for children online; and 4) Fighting against child sexual abuse and child sexual exploitation. The strategy proposes a series of actions to be undertaken by the Commission, Member States and the whole industry value chain[7]. The strategy was approved in 2012, a term for its implementation has not been established and it continues to be the key policy document on a European level that guides the states in the elaboration of their own policies in the field of child online safety.

One of the actions established for stimulating quality content online for young people is "digital and media literacy and teaching online safety in schools". The strategy established the obligation of the member-states to take the following actions:

- Step up the implementation of strategies to include teaching online safety in school curricula by 2013;
- Reinforce informal education about online safety and "provide for" online safety policies in schools and adequate teacher training;
- Support public-private partnerships to reach the above goals.

At the same time, the European Commission has assumed the following commitments:

- Support the identification and exchange of best practices among Member States in the areas of formal and informal education on online safety, the creation of relevant educational content, and public-private relationships aimed at reaching out to children, parents, teachers and carers;
- Develop a specific module within Europass for digital competence and improve the indicators for use and impact of ICT in education.

A Digital Agenda for Europe[8]

Although it is a rather complex policy document that aims to define the key enabling role that the use of information and communications technologies will have to play if Europe wants to succeed in its ambitions for 2020, it also regulates the obligation of Member-States to include online safety in schools. According to the actions planned, member-states of the European Union were meant to include online safety into the school curricula before 2013.

Digital Education Action Plan[9]

The priority of the European Commission to "Develop relevant digital competencies and skills for the digital transformation" also refers to online safety as one of fields that describe digital competency. One of the actions planned in this regard is to launch an EU-wide awareness-raising campaign targeting educators, parents and learners to foster online safety, cyber hygiene and media literacy.

This policy document highlights the importance of online safety and "cyber hygiene" in the context of developing digital competencies. The Action Plan recognizes the need to strengthen children's critical thinking and to develop their competencies, so they can analyse and overcome existing dangers. To do so, actions must be taken to raise awareness in educators, parents and learners about online safety.

European Framework DigCompOrg[10]

This framework represents a set of measures that

6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0196&from=EN

7 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0196&from=EN

8 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

9 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&from=EN #footnoteref21

10 https://ec.europa.eu/jrc/en/digcomporg

can be used by primary, secondary and vocational education institutions, as well as higher education institutions to guide a process of self-reflection on their progress towards comprehensive integration and effective deployment of digital learning technologies. The strategic vision of this framework refers to progressive and efficient integration of technologies into the educational process as an educational innovation that involves the planning of changes in three dimensions: pedagogical, technological and organizational.

DigCompOrg has 7 key-elements that are described using 74 descriptors. Online safety can be found in the description of several key-elements in this reference framework (Teaching and Learning Practices, Leadership and Governance Practices, Secure Infrastructure). In general terms, a "digitally competent" educational institution must meet the following conditions:

1. Have governance and leadership practices in the field, which involves having a well-developed management system for the integration of ICT into education and a plan for its implementation;
2. Have appropriate teaching and learning practices, focused on the development of digital competencies of the employees of educational institution and its students, but also readapt the roles and teaching approaches in the teaching-learning process;
3. Ensure the professional development of all employees in the educational institution at all levels;
4. Carry out practices of evaluation of efforts in the field;
5. Ensure quality content, including through the school curriculum that needs to be re-interpreted and updated in order to ensure the integration of digital technologies in the educational process;
6. Collaboration and networking between institutions relevant to the subject, with direct participation of students and teachers in the knowledge and experience exchange;
7. A planned digital infrastructure, subject to a specific management plan, to ensure the efficiency and optimal use of digital technologies in the educational process.

In terms of online safety, DigCompOrg establishes that[11]:

- Teaching and learning practices should primarily focus on safety, risks and responsible behaviours in the online environment;
- Digital infrastructure should comply with measures that protect the privacy, confidentiality, and safety of students. This could include legal obligations regarding data protection, and guides for employees and students regarding protection of privacy, confidentiality and safety in the online environment;
- Governance and leadership principles imply the existence of a policy for the integration of ICT into the institutional framework, policy that would define the positive ways of using ICT in the educational process. This organizational policy must include a chapter about online safety.

The European Digital Competence Framework for citizens DigComp[12]

The Digital Competence Framework identifies five areas of digital competence for citizens:

1. Information and data literacy;
2. Communication and collaboration;
3. Digital content creation;
4. Safety;
5. Problem solving.

In this competency framework, safety refers to the following aspects:

1. **Protecting devices**, digital content; understand risks and threats in digital environments. To know about safety and security measures and take those into account in order to ensure confidentiality and correctness of decisions made.
2. **Protecting personal data and confidentiality**; understand how to use and share personal information while being able to protect oneself and others from damages. To understand that digital services use a "Privacy policy" to inform how personal data is used.
3. **Protecting health and wellbeing**, which involves the ability to avoid health-risks and threats to physical and psychological wellbeing while using digital technologies. To be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying). To be aware of the use of digital technologies for social well-being and social inclusion.

11 *http://publications.jrc.ec.europa.eu/repository/bitstream/JRC98209/jrc98209_r_digcomporg_final.pdf*

12 *https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework*

4. **Protecting the environment** by being aware of the environmental impact of digital technologies and their use. Within DigComp, digital environment is the term used to describe the framework for performing digital actions, without referring to a particular technology or digital device.

DigComp established 8 proficiency levels, which are divided into 4 categories, and examples of applicability of these competences according to described scenarios[13]:

- Basic;
- Intermediary;
- Advanced;
- Highly specialised.

These standards help delimit measures of online safety from measures of online security.

DigComp was implemented differently in European states. The majority have integrated online safety into the digital competency normative framework, in the context of the elements regarding "Protecting personal data and confidentiality", but also "Protecting health and wellbeing"[14].

"Protecting personal data and confidentiality" is a competency that implies understanding the ways in which personal information is used and shared; understanding that digital services use a "Privacy policy" to inform how personal data is used, in order to help students protect themselves and others.

"Protecting health and wellbeing" represents another competency from the same category, its goal is to avoid health risks and threats to physical and psychological wellbeing while using digital technologies; develop competencies that would help students protect themselves and others from the potential dangers of the digital world (i.e. online harassment).

Recommendation of the Committee of Ministers on developing and promoting digital citizenship education[15]

Member states of the Council of Europe, including the RM, are encouraged to revise their legislation, policies and practices, to include a learning framework and ensure that it corresponds to the Recommendation of the Committee of Ministers on developing and promoting digital citizenship education[16].

"Digital citizenship education" is the empowerment of learners of all ages through education or development of competencies for learning and active participation in the digital society to exercise and defend their democratic rights and responsibilities online, and to promote and protect human rights, democracy and the rule of law in the online environment. Digital citizenship education promotes the development of a set of values, skills, attitudes, knowledge that would help the citizen participate actively and responsibly online, using digital technologies competently and positively.

This program is based on 3 key-pillars:

1. "Being online" (access and inclusion, learning and creativity, media and information literacy)'
2. "Wellbeing online" (ethics and empathy, health and wellbeing, online presence and communication);
3. "Rights online" (active participation, rights and responsibilities, privacy and security, consumer awareness)[17].

13 *https://publications.jrc.ec.europa.eu/repository/bitstream/JRC106281/web-digcomp2.1pdf_(online).pdf*

14 *https://eacea.ec.europa.eu/national-policies/eurydice/sites/eurydice/files/en_digital_education_n.pdf*

15 *https://eacea.ec.europa.eu/national-policies/eurydice/sites/eurydice/files/en_digital_education_n.pdf*

16 *Recommendation CM/Rec (2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education, adopted by the Committee of Ministers on the 21st of November, 2019, at the 1361st meeting of the Ministers' Deputies*

17 *https://rm.coe.int/10-domains-dce/168077668e*

1.2. Comprehensive approach model to online safety in schools

International policies and recommendations, especially the European Strategy for a better Internet for Children, mention a series of actions that should be taken for online safety in schools:

~ Include teaching online safety in schools;

~ Reinforce informal education about online safety;

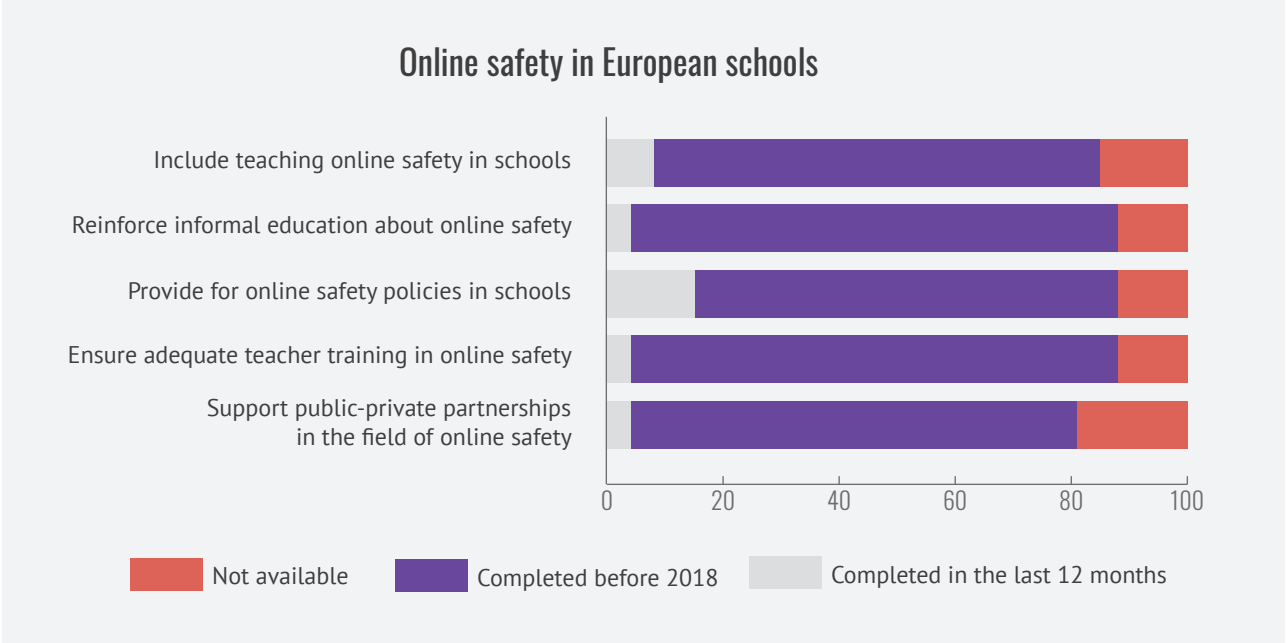
~ Provide for online safety policies in schools;

~ Ensure adequate teacher training in online safety;

~ Support public-private partnerships in the field of online safety;

~ Other relevant activities.

Figure 1: *"Online safety in European schools"* ***Source:*** *Report on the implementation of the European Strategy for a Better Internet for Children in the Member States of the European Union, 2018*[18].



These measures have been implemented by the majority of European states before 2018. In over 85% of states, online safety is taught in school. Besides regular activities carried out according to the school curriculum, 88% of states also carry out informal educational activities about online safety. Simultaneously, there are teacher training programs in these countries and public-private partnerships in the field of online safety are encouraged[19].

According to the Organisation for Economic Co-operation and Development (hereafter, OECD) all these determine a comprehensive approach to online safety in schools. This involves overcoming educational responsibilities and integrating online safety into all aspects of school activity, into all policies, procedures and processes in the educational institution. The school plays a key role in this context, its challenge being to empower children in order to reduce the negative use of the Internet and digital devices, while encouraging the use of ICT in the learning and teaching process and in establishing social connections[20].

This approach implies that both teachers, and other members of staff from the educational institution can recognize, respond and help children in risky situations related to online safety.

18 *https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7*

19 *https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7*

20 *https://www.oecd-ilibrary.org/docserver/f21353a9-en.pdf?expires=1589194601&id=id&accname=guest&checksum=90A761AF4E566F8D36E5B29545B2F5B8*

Thus, based on the above-mentioned information, several key-pillars of the online safety in schools policy start to take shape. The following is an example of how the UK put international recommendations into practice, by encouraging the development of institutional policies in the field. Similar elements can be found in the school policies of other states, too (Australia, Poland, etc.)[21]:

1. Policies and procedures that establish responsibilities for the whole school community:
   - ✔ Existence of an online safety in school coordinator, who is responsible for monitoring the implementation of policies in the field of online safety;
   - ✔ Institutional policies that refer to online safety integrated or linked to other existing school policies;
   - ✔ Intervention procedures and policies in cases of online abuse.
2. Communication with parents and carers about safety of children online:
   - ✔ Involve parents and carers in the process of developing school policies on online safety;
   - ✔ Inform parents about measures taken by the school to ensure a safe learning environment for children with the use of ICT;
   - ✔ Inform parents about online safety and providing materials, information, resources etc.
3. Developing teachers' abilities in the field of online safety:
   - ✔ All teachers who carry out activities on online safety are adequately prepared and have participated in trainings about online safety;
   - ✔ Online safety at pedagogical, technological and organizational level is included in the qualification courses for teachers, etc.
4. Developing students' abilities in the field of online safety:
   - ✔ Include the subject in the compulsory school curriculum;
   - ✔ Positive approach to educating safe online behaviours;
   - ✔ Compulsory to approach the risk of sexting;
   - ✔ Activities should be oriented towards reducing risks or dangers, but also towards discussions about the risks of certain online behaviours, to develop critical thinking skills in children etc.
5. Secure infrastructure that would allow the safe use of technologies:
   - ✔ Ensure efficient security systems, such as content filter programs, monitoring and firewall technologies or anti-virus systems, all supported by regular and detailed monitoring of the computer systems;
   - ✔ Documentation of all computers in the school that have access to the internet. In case of serious breaches, documentation of the network and hardware devices can help in the subsequent investigations. Particular consideration should be paid to the monitoring of mobile or wireless equipment etc.

21 *https://www.aoc.co.uk/sites/default/files/E_Safety_Developing_whole_school_policies_to_support_effective_practice.pdf*

Main findings in the international recommendations framework:

1. Integrating online safety into the educational process has been a priority of the European states over the last 10 years.
2. Online safety is one of the key-elements established by the European Commission in the Digital Competence Framework DigComp. This indicates the need to approach digital competency and the impact of technologies from a broader perspective: not just from a technological point of view, but also considering the impact that the use of technology has on the psychological wellbeing of children
3. The digitalization of the educational process cannot be perceived as a distinct dimension that ensures the emotional wellbeing of the child during the educational process. In the context of technological evolution and integration of technologies in the educational process, it becomes necessary and only natural to establish priorities for protecting children online. European policies and practices integrate online safety in all education digitalization trends, and this should be a key aspect in all national educational initiatives and policies.
4. The main actions recommended in international public policies refer to integrating online safety into the school curriculum from an early age, carrying out various information and awareness-raising activities for the school community (students, parents, teachers etc.) and developing institutional policies that would ensure an efficient response of the school to the challenges that children face online.
5. Online safety education should also approach subjects such as sending self-generated photographs and videos of a sexual nature.

2. The issues around child online safety

2.1. Interests and risks that children are exposed to online

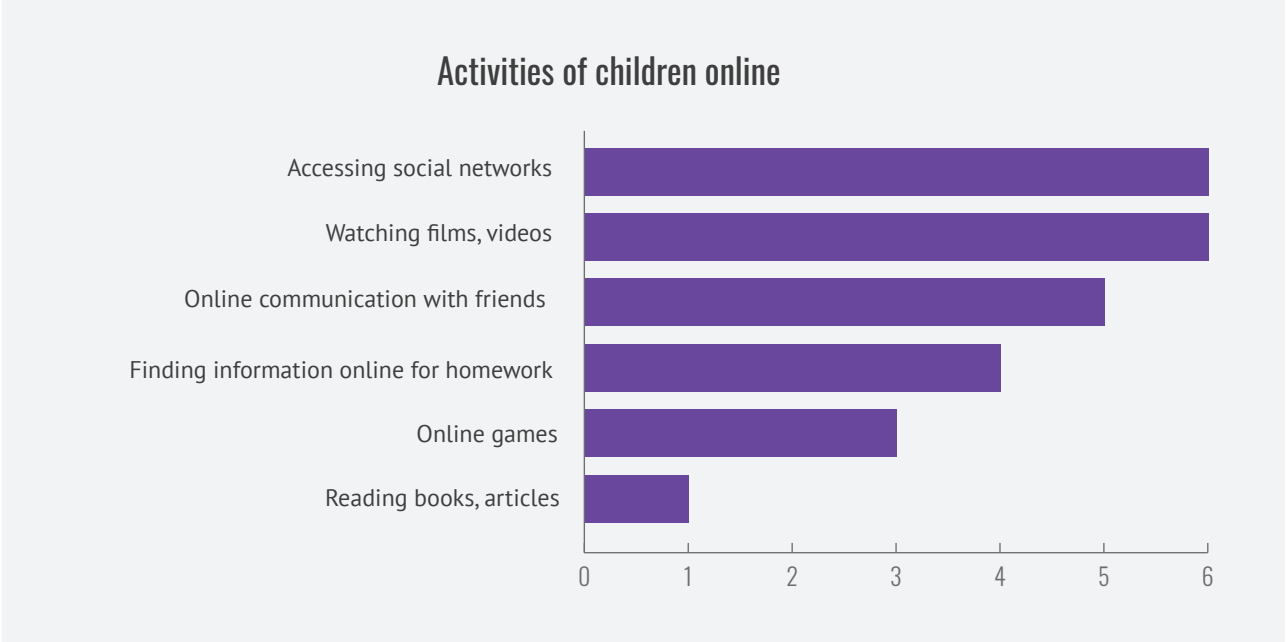
The most recent national study in the field of online safety[22] indicates some new trends in the behaviour of children from the Republic of Moldova. An increasing number of young children use the Internet before they even start going to school. In total, 96,5% of children aged 12 to 15 have an account/profile on social networks, and 44% of them have been present on social media from an extremely young age, before the age of 10. Thus, more and more children are present on social networks from an early age, they make new friends online – people they may not necessarily know in real life, exposing themselves to multiple risks that are associated with online interactions with strangers.

The same study shows that children aged 12-15 from the RM use the Internet for different reasons[23]:

- Educational (to do their homework, read informative materials, books etc.);
- Communication and socialization (access their social media accounts, talk on forums, chats, etc.)
- Entertainment (online games, watching vlogs, clips, films etc.)

Focus-group discussions with students/pupils re-confirmed the interest children have in social networks, films or videos and communicating with friends.

Figure 2: *"Most popular online activities among children"*
Source: *Results from focus-group discussions with students*



The risks that children are exposed to online can be conventionally divided into three categories[24]:

- **Content risks** – the child is recipient of mass distributed content. The actors involved are the child and the other people that generate online content.
- **Contact risks** – there is interaction between the child and an adult who initiated the interaction. The child is a passive participant, the adult initiates and controls the contact.
- **Conduct risks** refer to situations among peers. The child can be the actor who initiates the online situation or the aggressor.

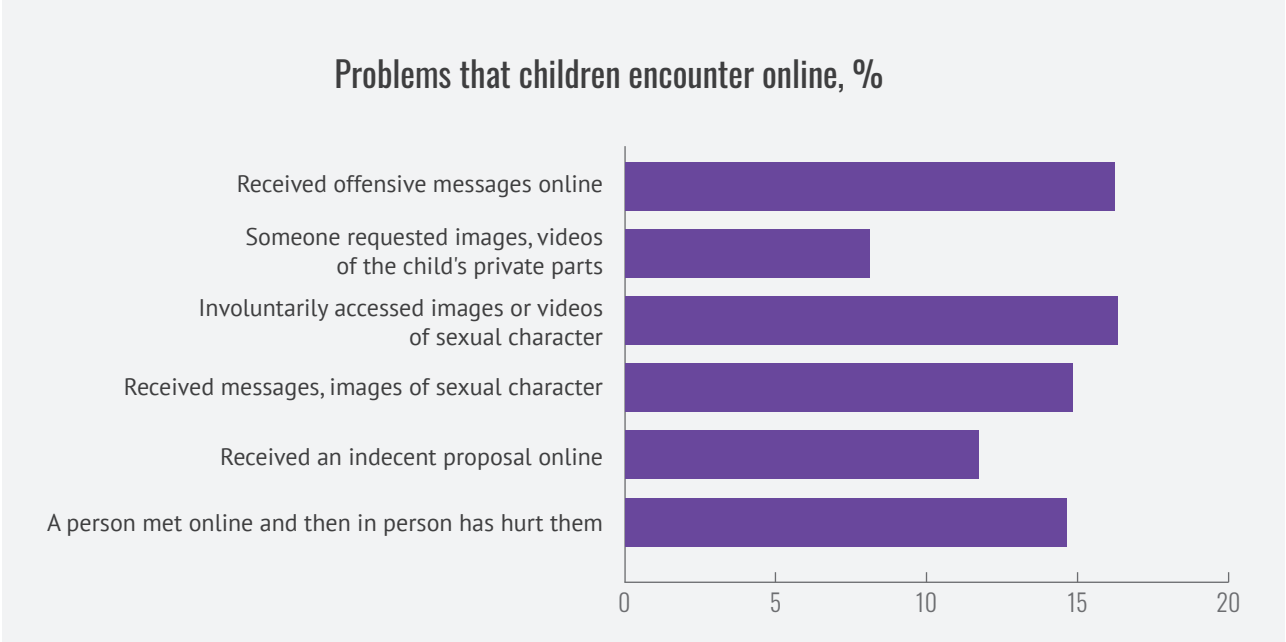
22 *http://lastrada.md/pic/uploaded/Child_Safety_online_ENG.pdf*
23 *http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf (RO)*
24 *http://eprints.lse.ac.uk/24368/1/D3.2_Report-Cross_national_comparisons-2nd-edition.pdf*

The most frequent **content risk** that children in the RM is exposed to is accessing content that promotes violence or sexual content. National statistics show that 16,3% of children aged 12-15 have involuntarily accessed videos or images of sexual character while they were browsing the internet, looking for information online. Most often, adolescents aged 15 encountered such situations (approx. 29,7% of the total number of children), the risk being lower for younger age categories (7,4% of the total number of children aged 12). However, because trends show that the use of Internet starts at an early age, it is necessary to consider these risks with respect to young children.

In terms of **contact risks**, we note grooming[25] situations that children are exposed to. Every 5th adolescent aged 14-15 has received photographs or videos with sexual content on the Internet, while 16,8% say they were asked to send such materials. National data state that the transmission/requesting of information of sexual character over the Internet comes from people that children know in real life, but also from people they only know online, and adolescents who received such materials have had more than one such experience[26].

Conduct risks refer especially to situations of online harassment, sexting and excessive exposure of personal information online. The most recent study on bullying in the RM shows that 70,8% of students in the RM have faced a situation of harassment, and 28,9% of these experienced cyberbullying[27][28].

Figure 3: *"Problems that children encounter online",*
Source: *Study "Child Safety Online", La Strada, 2017*



In the first semester of 2020, a 250% increase (compared to 2019) was registered in the number of requests from children that refer to contact risks and online interactions with other people. In 54% of cases, relationship problems are cases of cyberbullying, in 29% of cases, the problems refer to the relationships between adolescents, while 17% of cases refer to sexting (Figure no.4). 36 cases of online sexual abuse were reported by children during the same period – 3 times more compared to the same period last year.

These data indicate about the increasing number of unpleasant incidents that children encounter in the online environment[29].

25 *Grooming – process of enticement of a child, establishing an emotional relationship with the goal of abusing or sexually exploiting the child (according to the Lanzarote Committee, available at: https://rm.coe.int/168046ebc8*

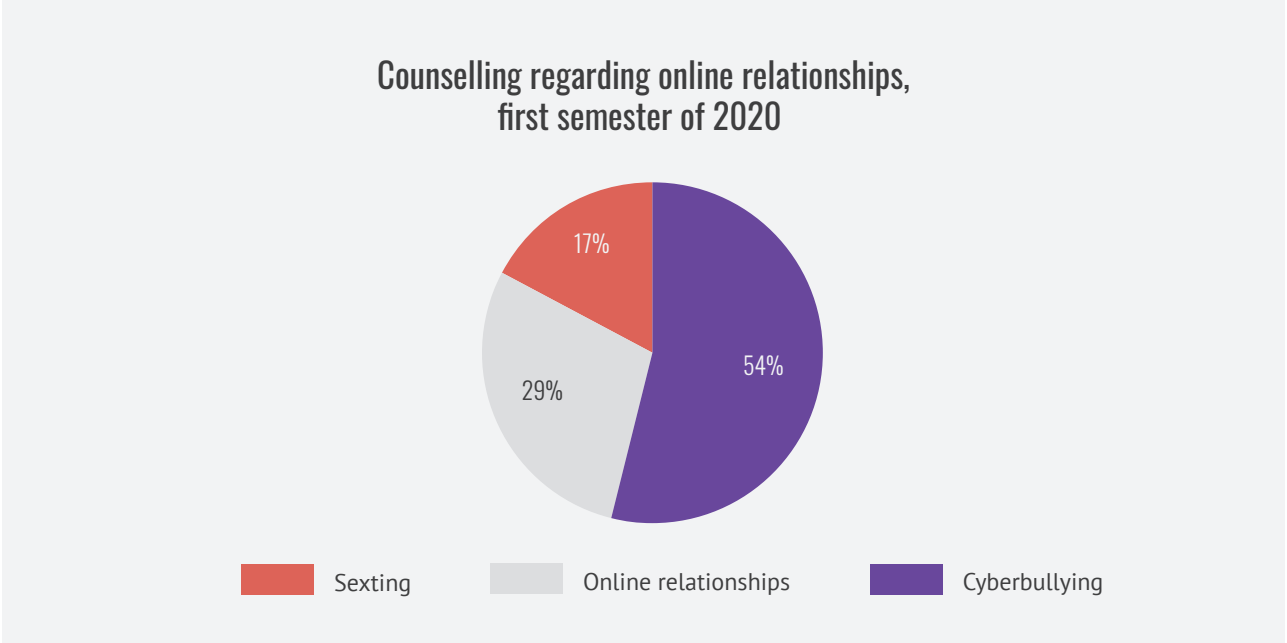
26 *http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf (RO)*

27 *Cyberbullying – online harassment*

28 *https://www.unicef.org/moldova/media/3146/file (RO)*

29 *http://lastrada.md/pic/uploaded/Siguronline%20Factsheet_%201st%20half%202020.pdf*

Figure 4: *"Categories of requests referring to online relationships on the www.siguronline.md platform, first semester of 2020",* ***Source:*** *La Strada Moldova*



2.2. Online safety from the students' perspective

What do children know about online safety

National research data in the field of child online safety state that every 5th adolescent aged 12-15 knows nothing about online safety. From what the children said, 81,9% of them know some things about online safety and they were told about some rules about online browsing by their parents, friends, teachers or from the internet. Although it may seem that they know online safety rules, they don't use them in practice and exhibit various risky online behaviours[30]. For others, online safety refers only to the security of their devices.

These findings were also confirmed by the focus-group discussions with students carried out for the purpose of this research. When discussing case studies, the children mentioned actions or reactions that go against the rules learnt. The responses of the students can be found in Table no. 1.

Table 1: *"Subjects discussed in lessons vs the attitudes of the students",*
Source: *Results from the focus-group discussions with children*

We shouldn't talk with unknown people online.	When asked about how they would react if they received a message from a person they don't know in real life, the children answered the following things: *"I would message them back, find out what they want".* *"Maybe he/she just wants to talk".* *"I would message them, so the number of my online friends doesn't decrease".*

30 *Child Safety Online, La Strada, 2017.*

On the internet, people may present themselves as someone other than who they are in real life.	Children reject the idea that people with hidden identities have suspicious interests, considering that they present no risk. *"It can happen, but it is very unlikely. That happens only in movies".*
When facing unpleasant online situations, we should ask for help from friends, parents, teachers or professionals.	When asked about what they would do if they were threatened online, children said that they would block that person. *"I wouldn't ask for anyone's help because no one can help, they can't prove anything and the online offers anonymity".*
We should not send intimate photographs.	When asked about how they would react in similar situations, children say that "*I would send such a photograph to the person I'm in a relationship with".*

All these situations point to the fact that following the activities and discussions on online safety carried out for students, children know the rules for online safety, but they don't have the necessary competencies/skills to be safe online. Thus, they continue to have reduced ability to act in the online environment, take responsible decisions and avoid dangerous situations. To develop children's' abilities, a change is required in the way the subject is approached, so that online safety activities don't only focus on teaching the rules for online safety, but also on empowering the children, on their ability to make correct decisions online.

Who would the children turn to if they had an online issue

If something unpleasant was to happen to them online, children aged 13-14 would first ask their parents for help, then their friends. Adolescents aged 15-16, however, would prefer to talk to their friends or a professional about it.

These differences are explained by age specific behaviours, namely the fact that during adolescence, children exhibit a stronger desire for autonomy and taking control over a situation, without the involvement of their parents. At the same time, this could also be the result of a poor relationship between the adolescent and the parents, or the lack of communication on sensitive subjects related to sexuality and online relationships.

Figure 5: *Figure no. 5 "Trustworthy people who students in the 6th grade would turn to in situations of online abuse"*
Source: *Results from focus-group discussions with children*

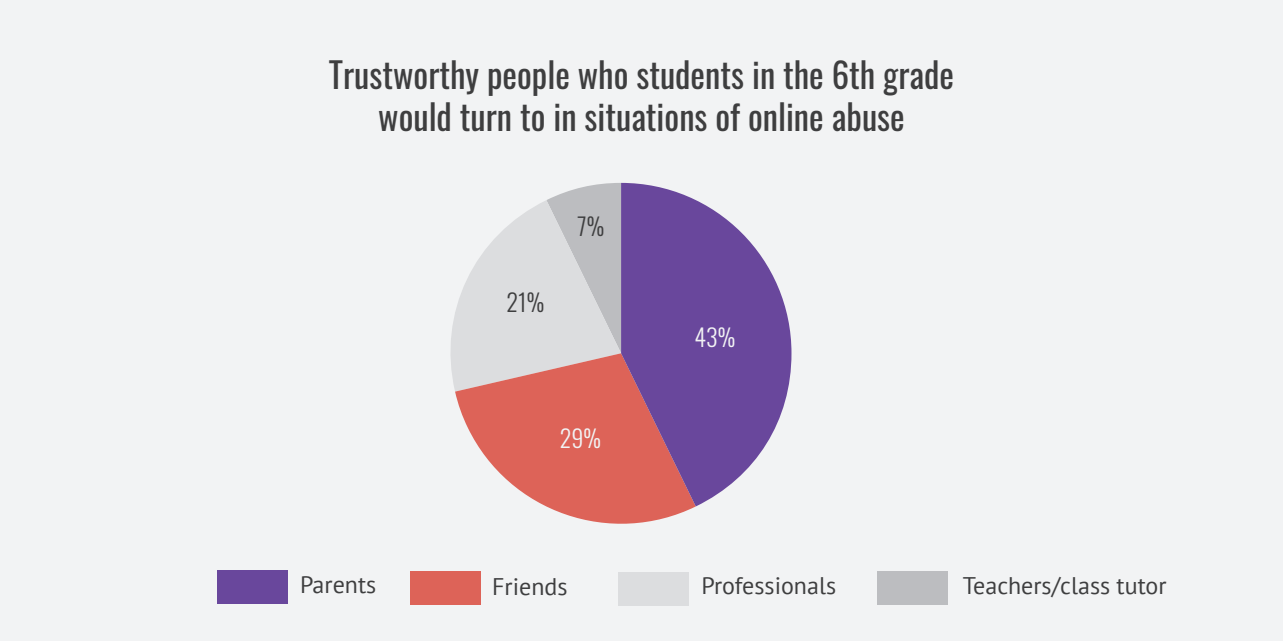
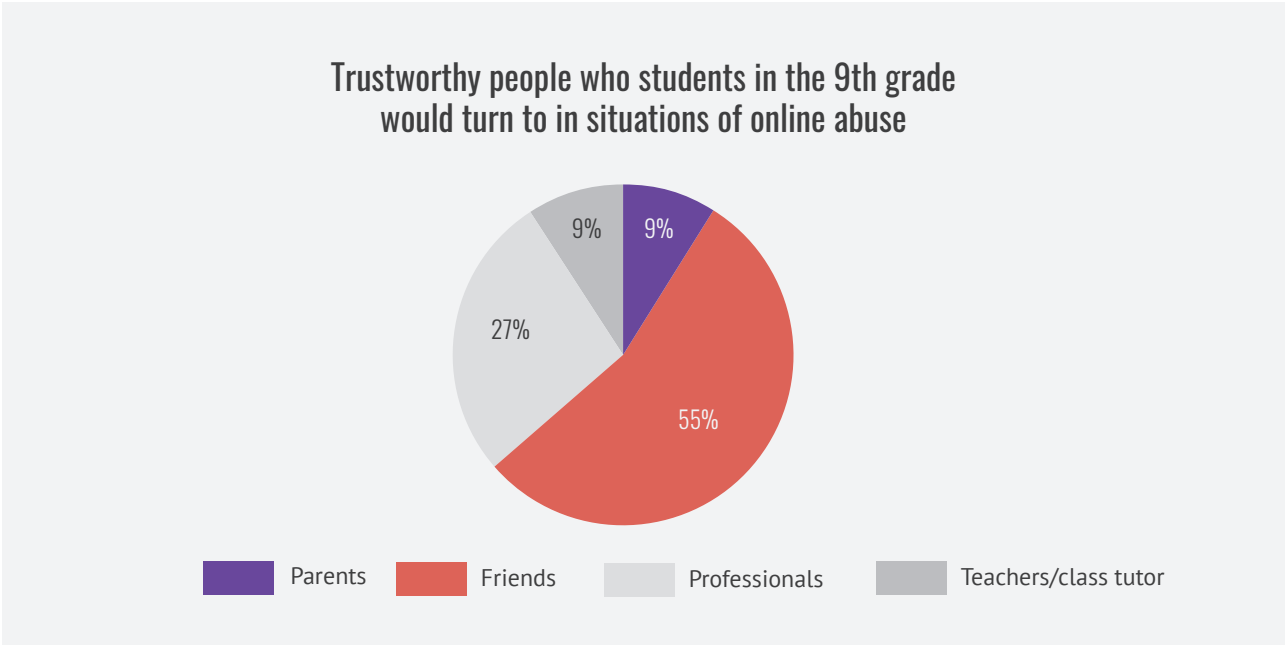


Figure 6: *" Trustworthy people who students in the 9th grade would turn to in situations of online abuse"*
Source: *Results from focus-group discussions with children*



In the last place, the children would talk to the class tutor or a teacher. Children don't trust teachers because of the following reasons:

"If the teacher knows, the whole school will know."

"If I tell a teacher about something like this, I'll have to listen to an hour of telling off."

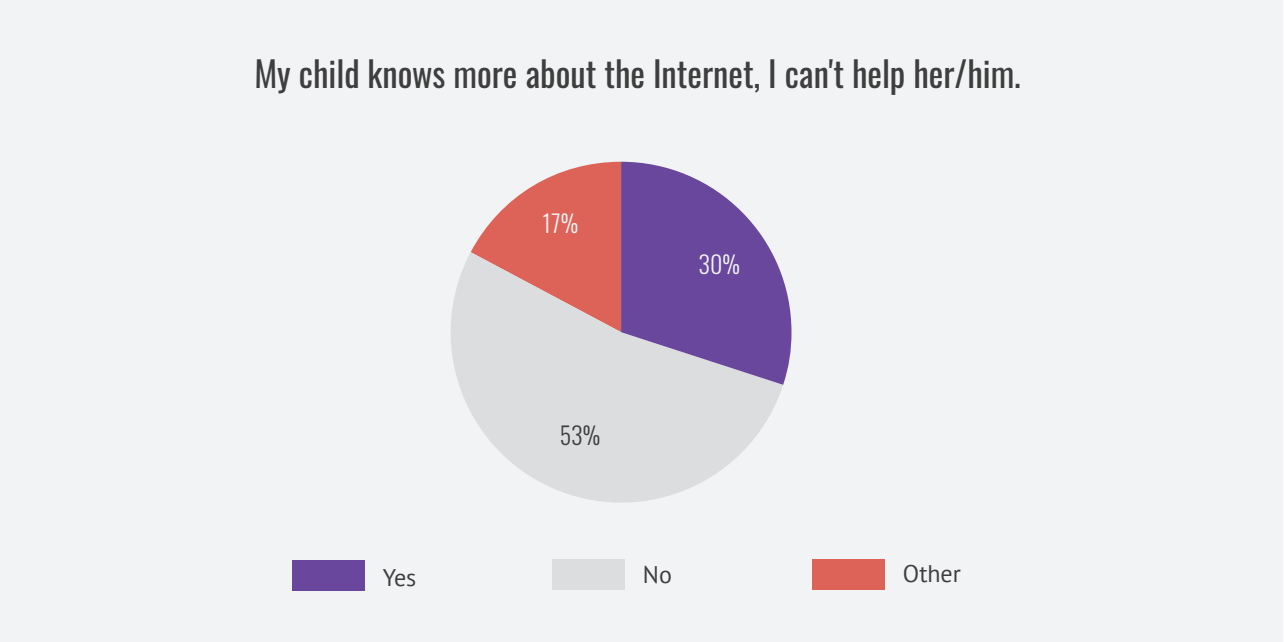
"They would immediately tell my parents. If I wanted them to know, I would have told them about it myself."

2.3. Online safety from the parents' perspective

What do parents know about online safety

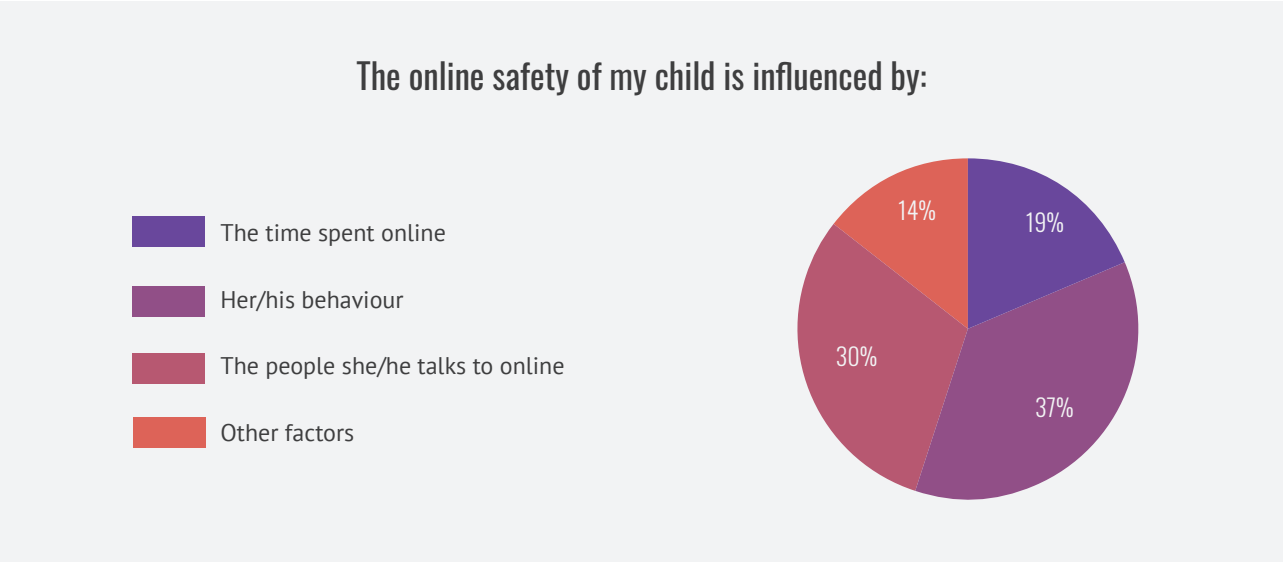
Parents from the RM have a vague understanding about what child online safety means and what they should talk about with their children. On one hand, parents consider that children are not well informed about how to correctly use the internet, which makes them worried. But on the other hand, parents don't know what to talk to their children about in order to avoid dangers and protect them. This fact often determines limitative reactions and restrictive approaches in education, some considering that it would be best if children do not have access to the internet.

Figure 7: *"Figure no. 7 "Parents' attitude towards the level of information of their children"*
Source: *Results from focus-group discussions with parents*



Parents have erroneous attitudes towards the time children spend online, thinking that this is the main problem in the children's relationship with digital technologies. This attitude makes parents limit the duration of the child's online activities, instead of focusing on positive parental mediation and educating safe online behaviours in their child. Other factors that influence the online safety of children are the environment (friends, classmates, society) and the school.

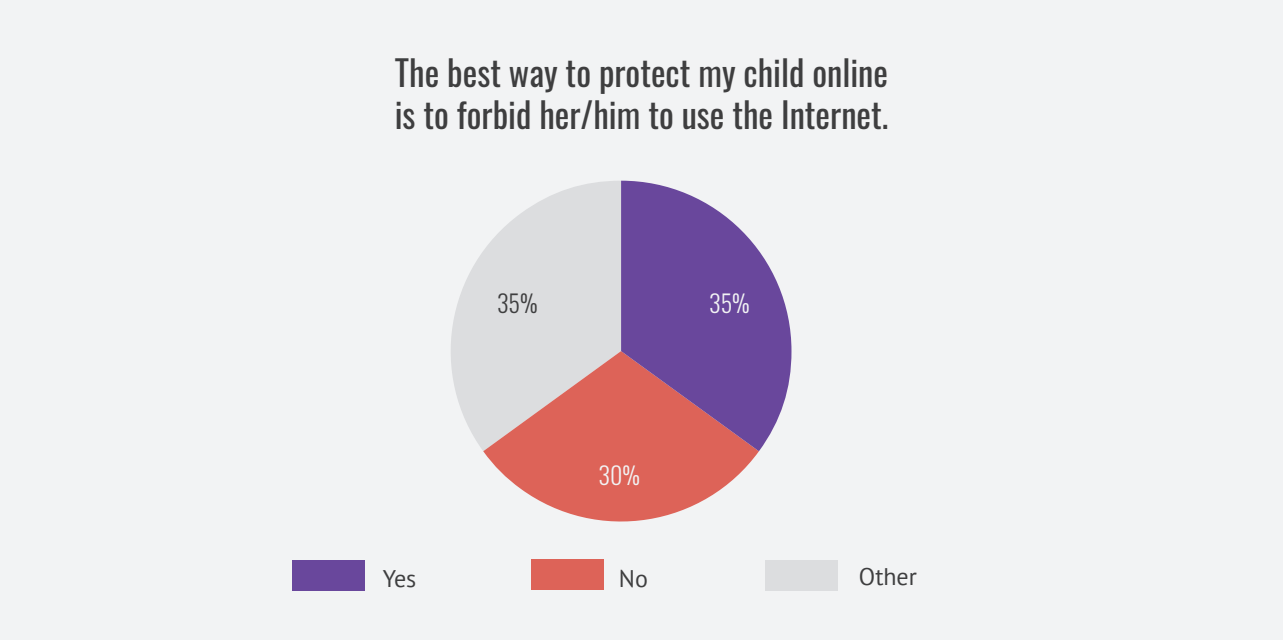
Figure 8: *Figure no. 8 "Factors influencing the safety of children online",*
Source: *Results from focus-group discussions with parents*



Parents' practices for educating safe online behaviours

The results from the focus-group discussions with parents show that 35% of parents consider that the best way to protect their child from online dangers is to forbid their access to the Internet, 30% are completely against forbidding the access, while the other 35% consider that there are better methods, such as supervision, control, or forbidding the access only to some pages (Figure no.9).

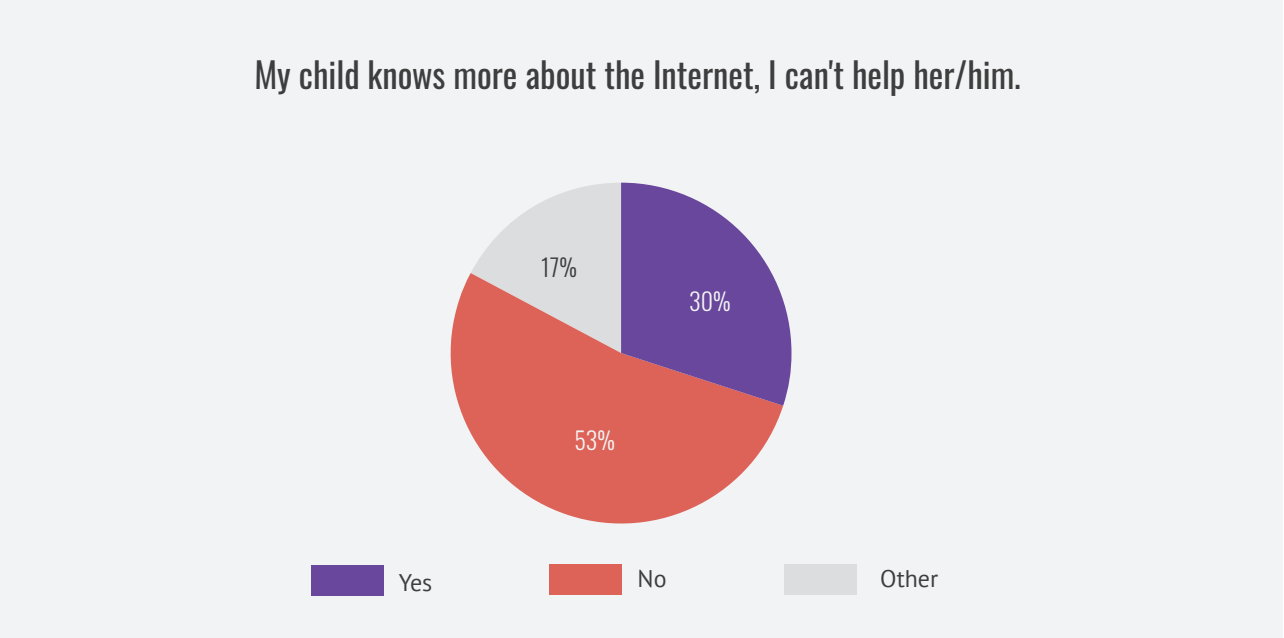
Figure 9: *"How do I protect my child online?",*
Source: *Results from focus-group discussions with parents*



One of the problems identified is the "generation gap" which determines a lack of communication and understanding in the parent-child relationship. Often, parents avoid talking to their child about the Internet and the child's activities online, because they don't perceive this as important in the education of their child. Children mention the misunderstandings between generations because they have different values, especially when it comes to social networks[31].

Moreover, there is a wrongful perception among parents on the children's level of information on online safety and the role they can have in guiding them. Many parents believe that children already know enough about the internet, and they can cope with internet problems by themselves (Figure no.10). Parents, who answered "Other" to the question, admitted that they are sufficiently informed themselves, but they realize that they should do something for the sake of their child's safety online.

Figure 10: *"The Children's level of information on online safety, in the perception of their parents",*
Source: *Results from focus-group discussions with parents*



31 *Child Safety Online, La Strada, 2017.*

2.4. Online safety from the teachers' perspective

What do teachers know about online safety

The results from focus-group discussions with teachers show that they don't clearly distinguish measures for online safety from measures for online security. When they carry out activities on online safety, they often refer and limit themselves to rules of using digital devices, setting strong passwords, anti-virus protection etc.

The level of professional training is influenced by the personal motivation of the teacher. In their opinion, it is usually young teachers who are motivated to take part in trainings about online safety. Teachers with more work experience don't have the digital skills to use information and communication technologies, they use the internet less frequently and that prevents them from perceiving the online environment as dangerous for its users, including for children.

"Teachers discuss the subject among themselves in meetings. There are teachers who are part of the Council for Child Rights Protection. They talk about this subject there."

Teacher

"We are only told when there are going to be activities organized."

Teacher

"Teachers are not trained. It is necessary for several teachers in the school to be trained on this subject, so they know how to correctly talk about it with children. It would be good if the teachers have a guide with the main terms and explanations and for it to be available on siguronline.md so every teacher can access it and study it."

Teacher

Although they don't have the appropriate professional training to approach online safety in their teaching activities, the majority of teachers who participated in the focus-group discussions have identified the following issues that the children from their schools have encountered:

Figure 11: *"Online problems encountered by primary school students",*
Source: *Results from focus-group discussions with teachers*

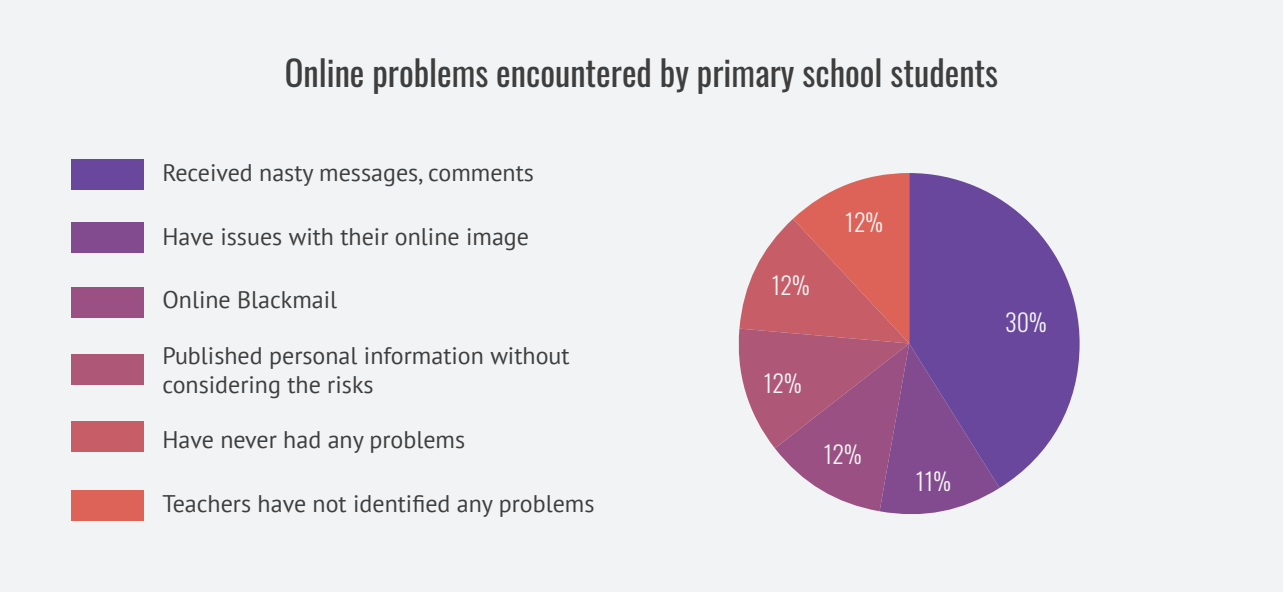
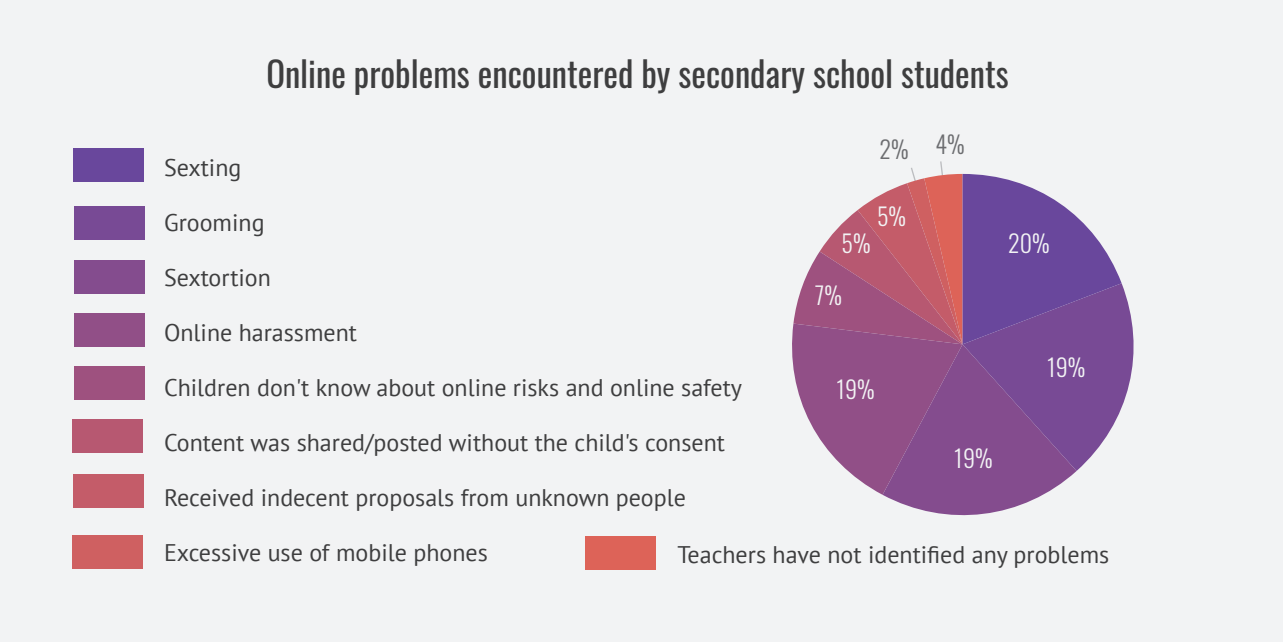


Figure 12: *"Online problems encountered by secondary school students",*
Source: *Results from focus-group discussions with teachers*



This data show that teachers, being in the front line, could find out about some cases of child online abuse, or they could notice risky or dangerous behaviours of children online. However, teaching activities on online safety mainly focus on digital security, and subjects such as online relationships, friendships, transmission of intimate photographs or online sexual blackmail are often avoided, even though these risks exist and adolescents are the most exposed to them.

Teachers' practices in the field of online safety

Often, teachers avoid to approach the subject of online safety in their teaching activities, preferring to involve external professionals. This happens for the following reasons:

- ✔ The subjects referring to online safety are complex and there is the risk of spreading erroneous information or a distorted message to the students;
- ✔ The subjects are sensitive and it is possible that some students will identify themselves in the case studies discussed;
- ✔ There is a lack of accessible resources and information in Romanian that would guide the teacher through the process of learning and teaching about online safety;
- ✔ The teacher's program is already overloaded, and thus, they don't have enough time to prepare for lessons and carry out these activities qualitatively;
- ✔ The negative attitude of the management of educational institutions towards extra-curricular activities and teachers involved in various initiatives;
- ✔ They don't feel comfortable discussing this subject, because they don't know how to solve all potential online problems and they are worried they wouldn't be able to answer all the questions students ask.

When asked about what they would need in order to be able to confidently carry out activities on online safety with their students, the teachers mentioned the following:

- ✔ They need a mentor from whom they can find out more information when they encounter issues or difficulties in the field of online safety;
- ✔ They need more time in order to be able to carry out the activities qualitatively;
- ✔ They need more training activities so that they feel prepared to approach the subject with students;
- ✔ They need teaching materials on the subject of "online safety".

"To make it easier to work with children, it would be good to have as many visual materials as possible. Various attractive posters. More videos. Other distribution materials. Teaching materials that include real case studies. This way, the child reads and finds out that such situations happened to someone real."

Teacher

Main findings regarding the issues around child online safety:

1. In the online environment, children are exposed to multiple risks, depending on their age, interests, knowledge and skills, but also depending on the presence or lack of trusted people who could guide them to safe online browsing. These risks concern both the content accessed by the child, and the people the child interacts with.
2. Although as a result of activities about online safety, children know the rules of safe online browsing, they do not have critical thinking skills, which determines them to take risks and act against the rules.
3. The level of involvement and information of the parents on the online safety of their children and the actions they can take as parents is minimal. This factor increases the level of vulnerability of the child in the online environment, because she/he is not being guided through her/his Internet experiences.
4. The level of professional training is influenced by the personal motivation of the teacher. Although many teachers avoid to approach the subject of online safety in activities with students, most often the teachers are those who notice risky behaviours of children online and know about some unpleasant experiences of the children. This fact reinforces the hypothesis that the school is the most suitable place and environment to develop critical thinking skills in children, and intervene and offer support to the children in situations of online abuse.

3. National policies and practices in Education

3.1. National public policy framework and normative framework

National public policy framework

Action Plan on promoting online safety of children and adolescents for the years 2017-2020

In 2017, child online safety became subject of a national action plan in the RM for the first time. It was then that the role of the authorities, public and private structures, and the non-governmental sector in promoting child online safety was recognized. By approving the Action Plan, the Education sector has taken up the commitment to organize regular information and awareness-raising activities for students about online safety, in the context of Safer Internet Day and Cybersecurity Month. Through this policy document, online safety was for the first time officially recognized as part of the extra-curricular, informal activities program carried out with students of all ages.

Things have evolved differently however, it has been determined that online safety would be approached not only as an extra-curricular activity, but also in the school program of the educational process. In the last 3 years, activities on online safety have been carried out for primary school students, secondary school students and high school students during compulsory and optional modules. In particular, we note the development of educational modules intended to contribute to the digital literacy of children, "Media education" for example – an optional module for secondary and high school students, or "Digital education" for primary school students.

Education Development Strategy for the years 2014-2020 "Education 2020"[32]

One of the directions of this strategy is the efficient integration of information and communications technologies (hereafter, ICT) into Education. In this regard, the following specific objectives were set:

- Objective 3.1 Enhance the access to quality education by providing educational institutions with modern equipment, useful in the educational process;
- Objective 3.2 Develop digital competencies by elaborating and putting into practice educational digital content;
- Objective 3.3 Increase the effectiveness and efficiency of the school management on the system, school, and classroom level through the use of information technology.

At the same time, we find that in the process of digitalization of the educational process, there were planned actions that would contribute to the safety of children online.

Normative framework

Education Code

Art. 135 para. j) from the Education Code establishes the obligation of teaching staff to inform students about all forms of violence and their behavioural manifestations, about individuals and institutions to whom they may address if they are subject to abuse. It is an express indication of the obligation of teaching staff to inform also students about the forms of online violence, new forms of online abuse, such as grooming, sextortion, cyberbullying etc; about how these are manifested and where they can get help in these situations.

Guidelines regarding the inter-institutional cooperation mechanism for the identification, assessment, referral, assistance and monitoring of child victims and potential victims of violence, neglect, exploitation and trafficking

The normative framework on child protection against violence in educational institutions is rather complex, being developed together with the approval of the Guidelines regarding the inter-institutional cooperation mechanism for the identification, assessment, referral, assistance and monitoring of child victims and potential victims of violence,

32 *Education Development Strategy for the years 2014-2020 "Education 2020" approved by Government Decision no. 944 from 14.11.2014.*

neglect, exploitation and trafficking[33]. Based on this inter-institutional mechanism, subsequently were developed institutional organization procedures and intervention procedures for the employees of the institutions in cases of abuse, neglect, exploitation, trafficking. These procedures generally refer to actions in the educational institution in the field of prevention and protection of children against violence, **without referring to the specifics of online abuse cases**.

The methodology for the application of institutional organization procedures **recommends carrying out activities with pupils about online risks as part of the primary prevention program aimed at children**[34]. In terms of the intervention procedures of the employees of educational institutions, they do not refer to situations of online abuse, and do not delimit the forms of abuse based on the way the abuse of the child was committed – with or without the use of ICT.

Thus, although the Government Decision no.270 from 08.04.2014[35] point 5.4 defines as child victim the child who, through actions or lack of, suffered psychological, physical or material damage as a result of violence, neglect, exploitation, including by means of information technologies, trafficking etc., specific actions for this type of abuse are not regulated and online abuse is not defined.

Guide for the implementation of the Child Protection Policy[36]

The guide for the implementation of the Child Protection Policy in schools includes a distinct chapter dedicated to rules for using the Internet and ICT in schools. On one hand, it is recommended to establish clear rules for the use of mobile phones, tablets, personal laptops, and the Internet, but also setting content control filters. Thus, this implementation Guide clearly establishes that it is the responsibility of the institution to ensure that the concerns regarding child protection are approached in the school policies on the use of the Internet and ICT.

Digital Competency Standards for primary school, gymnasium and lyceum students[37]

These Standards describe 10 key-competencies that should be developed in primary, secondary and high school pupils:

1. Use of computer systems;
2. Processing text documents;
3. Creating and editing images;
4. Elaborate, construct and display electronic presentations;
5. Processing data using spreadsheet calculations;
6. Use of Internet;
7. Online communication;
8. Elaborating and implementing algorithms;
9. Organizing and processing information using data management systems;
10. Respecting ethics and information security norms.

Although points 6, 7 and 10 could refer to some aspects of online safety, these actually directly refer to the use of technologies and information security. For example, point 6 refers to the following aspects: browsing the Internet, accessing web pages, finding information using distinct key-words, finding information using simple searching criteria, organizing and managing information downloaded from the internet etc.

Point 7 regarding online communication refers to the following sub-aspects: communication using digital telephony, social networks and instant messaging, creating and managing personal accounts in various online communication environments, using virtual spaces to create their own digital identity.

Point 10 "Respecting ethics and information security norms" refers to intellectual property (defining the notion of intellectual property, respecting copyright over digital information etc.), digital security (defining the notion of digital security, respecting the rules ensuring digital security, using means of ensuring digital security in real situations, etc.), digital ethics

33 *Government Decision no. 270 from 08.04.2014, regarding the approval of the Guidelines regarding the inter-institutional cooperation mechanism for the identification, assessment, referral, assistance and monitoring of child victims and potential victims of violence, neglect, exploitation and trafficking, published 18.04.2014 in the "Monitorul Oficial" journal no. 92-98, art. 297.*

34 *The methodology for the application of institutional organization and intervention procedures for the employees of institutions in cases of abuse, neglect, exploitation, trafficking approved through the Order of the Ministry of Education no. 858 from 23.08.2013.*

35 *Government Decision no. 270 from 08.04.2014, regarding the approval of the Guidelines regarding the inter-institutional cooperation mechanism for the identification, assessment, referral, assistance and monitoring of child victims and potential victims of violence, neglect, exploitation and trafficking*

36 *https://mecc.gov.md/sites/default/files/politica_de_protectie_a_copiluluighid_de_implementare.pdf (RO)*

37 *Digital Competency Standards for primary school, gymnasium, and lyceum students, approved through the order no. 862 of the Ministry of Education on 07.09.2015, available at: https://mecc.gov.md/sites/default/files/cnc4_final_competente_digitale_elevi_22iulie2015_1.pdf (RO)*

(defining the notion of digital ethics, respecting the rule of digital etiquette, promoting digital ethics norms etc.).

National standards do not approach aspects such as protecting the health and wellbeing of the child in the online environment or protecting personal data and privacy, understanding the ways to use and share personal information so that we can protect ourselves and others from dangers, as set out in the European Digital Competence Framework for citizens DigComp.

3.2. Practices of educational institutions in the field of child safety online

The practices promoting child safety online found in education institutions in the RM will be described and analysed in this chapter, from the perspective of their compliance with the European standards that define the Comprehensive Approach model to online safety in schools.

a. School governance

Institutional policy framework in the field of child online safety

Managerial plans

One of the good practices mentioned by the focus-group discussions is the inclusion of online safety into the managerial plan of the educational institution, according to the Extra-curricular activities Program elaborated by the Ministry of Education, Culture and Research (MECR). This allows a better organization of the activities, allocating enough time to prepare the thematic activities.

"There is the managerial plan. It is drawn up based on the Ministry plan. When the circulars come around, sometimes some subjects can be suggested to be approached (referring to activities in general). Technically, it is known from the beginning of the school year that in February there will be activities organized regarding the online environment."

Deputy director for Education

Other educational institutions organize activities about online safety only if there is a circular issued in this regard:

"We carry out activities during the periods mentioned by the circulars. The problem is that the circulars are issued 2 or 3 days before the activities are meant to be carried out. There isn't really time for qualitative preparation. The subject is approached superficially, to tick a box. We write a note for the Direction that X activities were carried out involving X students."

Deputy director for Education

Child Protection Policy

The Child Protection Policy is an institutional policy document that refers to the protection of children from any form of violence in the educational institution. According to the recommendations of the Ministry of Education, Culture and Research, it is the responsibility of every educational institution to ensure that the concerns regarding child protection are approached in the school policies on the use of the Internet and information and communication technologies. The Guide for the implementation of the Child Protection Policy in schools[38] includes a separate chapter dedicated to rules for using the Internet and ICT in schools, with the following recommended structure:

- Clear rules for using mobile phones, tablets, laptops, personal computers, video consoles;
- Clear rules for using the Internet;
- Establishing content control filters.

These however don't aim to empower the child to use technologies safely, don't establish indicators for identifying cases of online abuse and don't provide for early intervention actions, they are only limited to aspects referring to using technologies in school and securing Internet access by setting content filters.

From the 48 educational institutions that the focus-group participants work in, only in one of them exists a child protection policy that aims to protect children from all forms of abuse and create a safe environment in the school. However, the document does not include aspects related to the protection of children from online abuse.

38 https://mecc.gov.md/sites/default/files/politica_de_protectie_a_copiluluighid_de_implementare.pdf (RO)

Institutional regulations

The model regulation for the organization and functioning of primary, secondary and high education institutions, approved by the MECR does not establish any measures regarding child safety online. This normative act establishes some general interdictions that are meant to ensure an adequate functioning of the educational process, while protecting the psychological and emotional wellbeing of students and employees. These interdictions include:

- Point 11 c) "It is forbidden to engage in any activity that violates the general rules of morality and endangers the physical and mental integrity of students and employees";
- Point 147 g) "The class tutor is responsible for observing students' behaviour, including for the purpose of preventing abuse, neglect, exploitation of the child; and reporting presumed or confirmed cases of abuse";
- Point 190 h) "Students are prohibited from possessing and broadcasting obscene or pornographic material";
- Point 190 i) "Students are prohibited from using mobile phones during lessons, exams and competitions";
- Point 190 k) "It is forbidden for students to insult and use aggressive language and behaviour towards classmates and staff in the Institution".

This normative act does not indicate specific measures that refer to the safety of children online, protecting children from online risks or the obligation of the institution's employees to prevent or intervene in cases of online abuse.

In practice, the internal regulations can include aspects referring to the publication of images with children and provisions on the ways to use mobile phones in the educational institution. The results of the focus-group discussions point out the fact that other aspects of online safety are not usually reflected in the Regulation for the organization and functioning of the educational institution.

Coordinating activities on online safety in the educational institution

The current normative framework does not establish specific roles for coordinating activities that promote online safety in the educational institution. In all 48 institutions, the deputy directors for Education are responsible for organizing activities about online safety in their educational institution, because of their responsibilities to organize all extra-curricular activities.

"A circular is issued by the Direction of Education. The deputy director for education announces all class tutors and organizes a meeting. Together they draw up a plan of activities. The class tutors prepare some of the activities with the students."

Teacher

Teachers consult the deputy director for education when they face problems in carrying out activities or when they have identified some problematic situations that children are involved in online. Likewise, teachers can also turn to the: school psychologist, ANET coordinator, computer science teacher. However, the knowledge that computer science teachers have in the field of automatic collection, storage, processing, transmission or distribution of information using digital equipment is not sufficient to guide the other teachers in the field of child safety online, as online safety refers to online behaviours of children and is not reflected in the object of study of the Computer Science module.

In the majority of cases, deputy directors for education do not have any training in the field of online safety. Online safety is a subject taught in extra-curricular activities, therefore, the deputy director is not obliged to participate in trainings on the subject, although responsible for the coordination of activities on the topic.

"Usually, the deputy director for Education is the one responsible for carrying out these activities. The problem is that the activities are different every month. They are all organized more superficially. The deputy director for Education doesn't even have enough training to guide teachers on how to approach this subject in a more interesting way for children. Children like when subjects like that are approached outside lessons, when people from outside the school come to talk to them."

Deputy director for Education

The role of students in promoting online safety

In the focus group discussions, we did not identify practices promoting online safety in school involving students, on their own initiative, at the level of student councils. Usually, children get involved in activities on online safety at the initiative of the teachers, after they were asked to do projects. In one institution, secondary school students are involved in online safety teaching activities for younger children.

"Older children are involved in information activities about online safety for younger children."

Teacher

Teachers mentioned the need of involving students or external professionals in carrying out activities with children about online safety. They found that students have a more serious attitude when a person from outside of school talks to them about these subjects, and not their teacher.

b. Teacher training

Training teachers in the field of child online safety

Child online safety is not distinctly covered in the continuous teacher training programs. Several thematic modules and topics talk about aspects referring to the digitalization of the educational process and the integration of ICT into the educational process:

- Integrating ICT into the educational process;
- Advanced training technologies through ICT;
- Developing digital competencies of teachers;
- Introduction to the use of information technologies in education;
- Modern educational technologies and resources, etc[39].

A separate module on "User ethics and online security" is included in the Plan for continuous training of teachers and those in management positions elaborated by the State Pedagogical University "Ion Creanga" from Chisinau[40]. Also, specific modules of continuous training are organized in disciplines that include topics on online safety such as personal development, computer science, extra-curricular education or media education[41]. However, it is not clear what aspects of online safety are addressed in these continuous training activities or whether they are only aimed at online security.

"Teachers discuss the subject among themselves in meetings. There are teachers who are part of the Council for Child Rights Protection. They talk about this subject there."

Teacher

"We are only told when there are going to be activities organized."

Teacher

"Teachers are not trained. It is necessary for several teachers in the school to be trained on this subject, so they know how to correctly talk about it with children. It would be good if the teachers have a guide with the main terms and explanations and be available on siguronline.md so every teacher can access it and study it."

Teacher

c. Policies and procedures

In the institutions where we conducted the focus-group discussion, there is a lack of intervention procedures in the case of online abuse. The majority of teachers declare that they haven't directly encountered cases of online child abuse, therefore they don't know what actions should be taken in such situations.

"I have spoken to the girl. She deleted the photographs. She understood that things could have gotten uglier and everything calmed down."

Teacher

Unfortunately, though, these situations can't always be solved just by getting the child to delete the photographs. Once the photos are sent, they can be seen by other people and can even end up shared on social networks, becoming available for anyone to see. With every view, the child is exposed to repeated victimization, making him/her relive all the negative emotions of the abuse. Also, once these photographs are viewed by classmates, the photos may be shared with other people too, the child could be made fun of, or even bullied online.

Although there is an inter-institutional mechanism in place for the identification, assessment, referral, assistance and monitoring of child-victims and presumed victims of violence, neglect, exploitation and trafficking, the teachers had contradictory opinions about applicability of the existing inter-institutional mechanism[42] in cases of online abuse. Some teachers believe that the same procedures relevant in all cases of abuse should be followed in situations of online abuse. Others completely rejected

39 https://mecc.gov.md/ro/content/centre-de-formare-continua-0 (RO)

40 https://mecc.gov.md/sites/default/files/universitatea_pedagogica_de_stat_ion_creanga_din_chisinau_0.pdf (RO)

41 https://mecc.gov.md/sites/default/files/universitatea_de_stat_din_moldova_0.pdf (RO)

42 Government Decision no. 270 from 08.04.2014, regarding the approval of the Guidelines regarding the inter-institutional cooperation mechanism for the identification, assessment, referral, assistance and monitoring of child victims and potential victims of violence, neglect, exploitation and trafficking

the idea of applying the same tool, specifying that existing procedures can't be applied in cases of online abuse because they don't take into account the specifics of these cases and don't provide sufficient tools and clarity for teachers in what actions they should be taking.

"It is difficult for teachers to talk to children about such situations. They don't know what is the best way to proceed."

Teacher

Teachers also mentioned other challenges:

- Indifference of other colleagues (teachers), which determines them not to get involved and not offer help/support to the child;
- Stereotyped attitudes towards online sexual abuse cases, which may determine them to blame the child for everything that happened to them and act against the child's best interests;
- Not knowing the signs of a potential online sexual abuse, or neglecting unpleasant situations that happened to children online and which aren't perceived as forms of abuse, which could determine them to be indifferent in such cases.

"We definitely need more resources and clarity in what we can do when these situations happen to children."

Teacher

At the same time, in the discussions with the specialists from the Psycho-pedagogical Assistance Service, but also with the school psychologists regarding the cases of online sexual abuse, it was found that they have a low level of information on this subject. The specialists are scared to intervene in these situations because they don't know exactly what to do so they don't harm the child. They admitted that the reason for their inactions is the lack of clear instructions in this regard. Social workers, guardianship authorities and the police are also affected by the lack of clear instructions, they encounter difficulties in the identification of cases and appropriate intervention. Similarly, the lack of knowledge about the specifics of online abuse, the elements that should be taken into account, how the abuse unfolds and evolves and the possible consequences of online abuse, all create impediments in ensuring an effective response from specialists in the field.

d. Parental involvement

There are no parental education programs in the field of child online safety, that would take into account the developments in the digital age, the risks that children are exposed to and the essential information that parents need to know to protect their children from online risks.

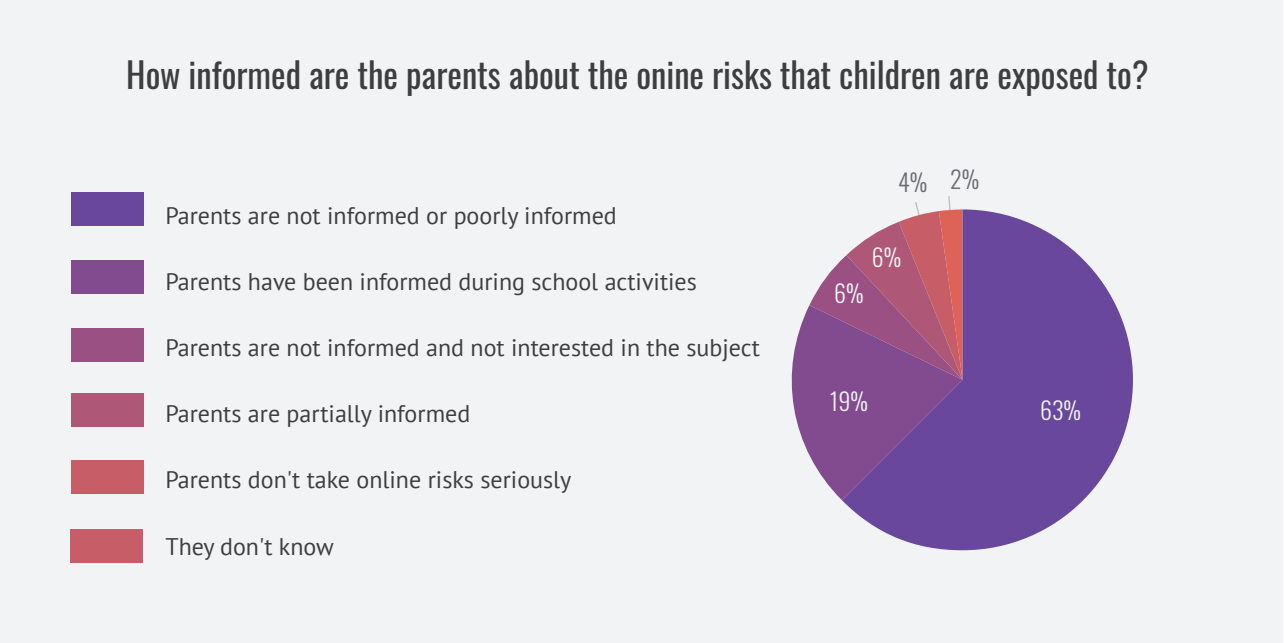
Information activities for parents about online safety are organized sporadically. Only one teacher mentioned that they have never spoken to parents about this subject and they don't know if in the school where they teach there were activities for parents organized on the subject.

"At meetings, we tell the parents to take notice of what their children do online."

Teacher

Often, parents don't know about the online risks that their children are exposed to. As a result, they don't know how to deal with them, but they don't do anything to change that either, passing this responsibility onto the teachers (Figure no. 13).

Figure 13: *"The parents' level of information about online risks",*
Source: *Results from focus-group discussions with teachers*



One of the challenges that teachers face when organizing information activities for parents is the lack of teaching resources, informative leaflets or other distribution materials for parents. Another challenge is the fact that many parents are abroad, and the children are cared for by their grandparents. The level of information and understanding of grandparents about what the Internet is, what the child does online and what the risks are is minimal. In such cases, the child usually has the freedom to browse the internet however much he/she wants, without limitations and without ensuring a safe online experience.

The parents' attitudes and involvement in educating safe behaviours online are different depending on the age of the children. The majority of parents of younger children (7-10 years old) are open and interested in collaborating to teach their child how to browse the internet safely.

Parents of secondary school students however, have a high level of resistance towards the subject and don't acknowledge the contact or conduct risks that their children may be exposed to online. Multiple teachers encountered the problem of parental disinterest towards online safety in parents' meetings, because they are sufficiently informed and don't need any more such information. Some parents believe that their child doesn't have access to the Internet and therefore isn't exposed to the danger.

"At the parents' meeting we discuss online safety. But they are not interested and don't pay attention either. They think that as long as it didn't happen to their child, the information isn't for them."

Teacher

e. Online safety education

Online safety is addressed in discussions with students both in compulsory and optional subjects, and in the context of Safer Internet Day or Cybersecurity Month. Subjects referring to online safety can be found across several compulsory and optional disciplines (See Appendix no.2):

- Personal development (primary, secondary and high school);
- Media Education (primary, secondary and high school);
- Digital Education (Primary school).

Often, subjects referring to online safety are integrated in modules or topics that refer to online or cyber security. For example, for the discipline "Technological education", primary school, 4th grade, the authors have proposed the following content topics for the "Digital Education" module, lesson "Good manners and digital correctness":

- Digital resources on web pages: who is the owner? In what way do we have the right to use them?
- Communicating using digital devices – some simple rules.
- And again, about dangers – computer viruses.

Although the name of the lesson suggests aspects related to online behaviours, the proposed content actually refers to cyber security, which creates further confusion between the subjects and aspects. In addition, the message conveyed is that if taking online security measures, that would be enough to avoid any online dangers.

Teachers carry out activities with students also within the Extra-curricular activities Program[43], in the context of Safer Internet Day and Cybersecurity Month. These activities are recommended by the Methodological indicators regarding the organization of the educational process for the Computer Science discipline for the school year 2019-2020[44].

According to these methodological indicators, during the Computer Science discipline, it is recommended to train in students **attitudes and habits of responsible behaviours, in order to prevent risky situations and promote a safe use of technology, safe Internet browsing etc.** Even so, lessons in the secondary and high school curriculum only refer to online security and cybersecurity[45].

f. Secure technologies and infrastructure

The Minimum Standards for equipping primary, secondary and high schools with ICT means establish the obligation of educational institutions to have specialized software to filter content on the Internet[46]. Although the obligation to have specialized software to filter content on the Internet in primary, secondary and high schools is regulated, this norm is not particularly known about. Discussions with the management of educational institutions show that these minimum standards for equipping schools with ICT are not put into practice.

More than 50% of schools (from the total of 48) have internet access through a wi-fi network. In all the cases, the access is restricted, which means a password is required to access the internet. Only in 3 institutions children have free access to wi-fi. Only in one institution, online content filters were set. We found that teachers did not know about the possibility of setting technical measures to filter content, believing that securing the access just meant setting an access password.

"Content filters aren't even installed in the computer classroom. We've had cases when images inappropriate for the pupils' age popped up on the computer screens."

Teacher

"There are no filters. It would be a good option, but they would still access that content, if not in school, then somewhere else."

Management staff

"The Ministry must take action with all service providers, so they are obligated to offer schools these filter settings."

Management staff

"It wasn't known. We weren't told. It would be good to hold accountable all those who provide such services."

Management staff

43 *MECR Order no. 1619 from 10.12.2019 regarding the approval of the Extracurricular activities Program in primary and secondary education, cycle I and II.*

44 *MECR Order no. 1046 from 21.08.2019 for the approval of Methodological Indicators regarding the organization of the educational process for the Computer Science discipline for the school year 2019-2020.*

45 *https://mecc.gov.md/sites/default/files/informatica_gimnaziu_ro.pdf (RO)*

46 *MECR Order no. 581 from 24.06.2015 regarding the approval of the Minimum Standards for equipping primary schools, gymnasiums and lyceums with ICT means.*

Main findings regarding national policies and procedures:

1. According to the Education Code, one of the main responsibilities of teaching staff is to inform students about all forms of violence, including domestic violence; about how these actions are manifested and what people and institutions they can turn to when they are subjected to an act of online abuse.
2. Child online safety is not a priority in educational policy documents, being regulated as a subject of extra-curricular activities' program and informal activities with pupils of all ages. Although the subject is included in the curriculum for compulsory and optional modules, there still persists a confusion in the terminology used and the subject approaches, often the term "online safety" being used instead of "online security" and vice versa.
3. The Digital competency standards for primary, secondary and high school students, approved by MECR in 2015, do not comply with the Reference Framework DigComp, recommended EU-wide. Online safety is not specified in national standards, although EU-wide, this is one of the key digital competencies.
4. The current normative framework does not regulate the ways to identify cases of online abuse in school, neither the intervention procedures for teachers. Practice shows a common trend among school psychologists and teachers of reacting and intervening intuitively, based on their own life experience and guided by their own attitudes and perceptions of the subject.
5. Teachers acknowledge the topicality of online risks for the physical and psycho-emotional safety of the child. At the same time, it is not clear to them what they should do to reduce these risks and what the role of the educational institution or teaching staff is.
6. Due to the lack of a parental education program, adjusted to the role of parents in the digital age, the subject is approached sporadically with parents. Teachers require thematic resources and trainings on the methods of communication and collaboration with parents about child online safety.
7. More than 90% of the educational institutions where we conducted the focus-group discussions for the purpose of this research, don't have specialized content filtering software, to filter the content that children can access through the school wi-fi. Educational institutions are not informed about their obligation to have these measures which are regulated by the normative framework, and they lack control measures from the MECR for their implementation.
8. There is no genuine participation of children in activities promoting online safety in schools. Usually, student involvement implies doing projects at the teacher's initiative. There were no direct involvement practices identified – through a student council or other – in improving the policy framework referring to online safety in schools or the relevant practices.
9. Teachers and school psychologists are poorly informed about online sexual abuse, how they can identify such abuses and how to intervene in such cases. Moreover, focus-group discussions point out a high level of stereotypes and reluctance towards the subject, which stimulates the blaming of the child.
10. Existing intervention mechanisms are not adjusted to abuses committed with the use of ICT. Teachers stated the need of elaborating specific procedures for cases of online abuse, that would explain the signs of this form of abuse and intervention recommendations, appropriate to the specific risks of these cases.

Main conclusions and recommendations

Conclusions

Regarding the national educational policy framework

1. The main recommended actions in international public policy frameworks refer to the integration of online safety into the school curricula from a young age; organization of various information and awareness-raising activities for the school community (students, parents, teachers, etc.) and developing institutional policies that would ensure an efficient response of the school to the challenges that children face online.

2. Child online safety is not a priority in educational policy documents, being regulated as a subject of extra-curricular activities' program and informal activities with pupils of all ages.

3. The Digital competency standards for primary, secondary and high school students, approved by MECR in 2015, do not comply with the Reference Framework DigComp, recommended EU-wide. Online safety is not specified in national standards, although EU-wide, this is one of the key digital competencies.

4. The current normative framework does not regulate the ways to identify cases of online abuse in school, neither the intervention procedures for teachers. Practice shows a common trend among school psychologists and teachers of reacting and intervening intuitively, based on their own life experience and guided by their own attitudes and perceptions of the subject.

Regarding the practices of educational institutions in the field of child safety online

5. Child online safety is not present in institutional policies, regulations for the organization and functioning of educational institutions, or in child protection policies. At present, there are only some recommendations of integrating the subject in child protection services, but these recommendations have not been implemented yet.

6. Activities educating safe online behaviours in students are organized chaotically, sporadically, the subject being often confused with activities about online security or cyber-security. The way the subject is approached often involves teaching some rules about online safety, which does not contribute to the development of skills and competencies. These activities are organized chaotically and superficially, usually in the context of "Safer Internet Day" and "Cybersecurity Month".

7. Teachers acknowledge the topicality of online risks for the physical and psycho-emotional safety of the child. At the same time, it is not clear to them what they should do to reduce these risks and what the role of the educational institution or teaching staff is. The involvement of teachers in promoting online safety depends on the level of motivation and understanding of the subject. At the moment, teaching activities about online safety aren't perceived as prevention activities for online abuse or as an opportunity to develop children's resilience to abuses.

8. Collaborating with parents in promoting child online safety is inefficient. Often, teachers face resilience from parents who don't acknowledge the actuality of the subject, reject the idea that the child is vulnerable online or believe that they don't need to be informed on this subject. Due to the lack of a parental education program, adjusted to the role of parents in the digital age, the subject is approached sporadically with parents. Teachers require thematic resources and trainings on the methods of communication and collaboration with parents about child online safety.

9. More than 90% of the educational institutions where we conducted the focus-group discussions for the purpose of this research, don't have specialized content filtering software, to filter the content that children can access through the school wi-fi. Educational institutions are not informed about their obligation to have these measures which are regulated by the normative framework, and they lack control measures from the MECR for their implementation.

10. There is no genuine participation of children in activities promoting online safety in schools. Usually, student involvement implies doing projects at the teacher's initiative. There were no direct involvement practices identified – through a student council or other – in improving the policy framework referring to online safety in schools or the relevant practices.

11. Teachers and school psychologists are poorly informed about online sexual abuse, how they can identify such abuses and how to intervene in such cases. Moreover, focus-group discussions point out a high level of stereotypes and reluctance towards the subject, which stimulates the blaming of the child.

12. Existing intervention mechanisms are not adjusted to abuses committed with the use of ICT. Teachers stated the need of elaborating specific procedures for cases of online abuse, that would explain the signs of this form of abuse and intervention recommendations, appropriate to the specific risks of these cases.

Recommendations

Revising the national digital competencies framework

~ Update the digital competencies framework for students, in order to integrate online safety into the digital competencies' spectrum, according to the European recommendations in the field;

~ Commit to and adopt the European Standards for Digital Competencies DigComp in educational institutions.

Integrating online safety in institutional policies

~ Elaborate a model institutional policy in the field of child online safety and encourage the development of such policies by every educational institution;

~ Elaborate detailed instructions that would meet the needs of teachers in better understanding how to protect children from abuse in the online environment, through effective prevention, protection and assistance actions;

~ Ensure the development of online safety policies through a participatory process, involving students and parents in dialogues about the improvement of institutional policies, procedures and processes on online safety in schools;

~ Create a Committee specialised in online safety in every school, that would guide the carrying out of online abuse prevention activities, the process of elaboration of an intervention plan in cases of identified cases of abuse etc.

Developing the skills of educational actors in the field of child online safety

~ Integrate child online safety into continuous training programs for teachers, school psychologists and staff from the Psycho-pedagogical assistance service;

~ Establish the obligation to participate in training courses in the field of child safety online, for all teachers who carry out activities on this subject within the compulsory or optional modules;

~ Training of deputy directors for education in the field of child online safety, in order to ensure an effective coordination and guidance of teachers at the institutional level, by a specialist trained in this field;

~ Integrate child online safety into parental education programs, and carry out regular information activities for parents about child safety.

Encouraging informal activities promoting child online safety

~ Continue running activities with students about online safety, in the context of Safer Internet Day, through the MECR circulars. Evaluate the opportunity of encouraging the management staff from educational institutions to include the subject in managerial plans, in order to streamline the process of organization and carrying out of the activities by the class tutors;

~ Include the Child Online Safety Competition into the Extra-curricular activities' program for primary and secondary schools, cycle I and II - activity that encourages the participation of teachers and students in promoting online safety within the educational institution and at national level.

Creating an implementation and monitoring mechanism of the ICT infrastructure in schools

- Elaborate new methodological indicators in collaboration with representatives from the ICT private sector, about how to implement the obligation to install a specialized content filtering software, by regulating the responsibilities of each party involved;
- Monitor the implementation of the normative framework that regulates the obligation of primary, secondary and high schools to have a specialized content filtering software by creating a mechanism for the periodic reporting of achievements in this regard.

Revising and adapting the intervention procedures in cases of online abuse in school

- Analyse to what extent the intervention procedures for ANET cases are relevant in cases of online abuse. Depending on the results of this analysis, it is recommended to adjust the ANET[47] instructions by specifying that they are also applicable in cases of online abuse, or to develop new distinct instructions for cases of online abuse;
- Organize training activities for teachers on the prompt identification and efficient intervention in cases of online abuse;
- Carry out ongoing training activities for the Psycho-pedagogical assistance service specialists, about the counselling and psycho-pedagogic support they can provide to children-victims of online sexual abuse;
- Ensure the collaboration between teaching staff and other community actors (NGOs, police etc.) from the moment of identification of the online sexual abuse in the institution, to ensuring a well-coordinated intervention, based on the child's needs.

47 *Abuse, neglect, exploitation, trafficking*