Reports
Country profiles

ITUPublications

National child online safety assessment for Georgia

2019

Acknowledgements

This report was prepared by International Telecommunication Union (ITU) experts David Wright and Boris Radanović, with the support and guidance of the ITU Office for Europe, under the ITU regional initiative for Europe on enhancing trust and confidence in the use of information and communication technologies. ITU would like to express sincere gratitude to the representatives of Ministry of Economy and Sustainable Development of Georgia for the support and assistance they provided to the ITU experts.

ISBN

978-92-61-28911-9 (paper version)

978-92-61-28921-8 (electronic version)

978-92-61-28931-7 (EPUB version)

978-92-61-28941-6 (MOBI version)

Please consider the environment before printing this report.

Table of Contents

List of Tables and Figures

Tables

Figures

Executive summary

Protecting children is everyone's responsibility. The establishment of a national strategy that drives coordinated activities for child online protection is an imperative given the variety and complexity of actors, technologies, and agencies as well as opportunities and threats.

Preparatory desktop research and a series of online surveys were organized in cooperation with the Ministry of Economy and Sustainable Development of Georgia. Interviews were completed with a range of stakeholders that play an important role on the field of child online protection. The following key challenges and recommendations is provided by ITU and South West Grid for Learning (SWGfL) to support the development of a national child online protection strategy for Georgia.

In terms of the primary challenges, it was concluded that:

- There is a low level of public awareness of online risks to children with a need to educate the general public on global online threats and opportunities.
- Parents, as well as specialists and professionals working with children, do not have a proper level of support, understanding and knowledge of child online protection issues and dangers.
- Online bullying is a significant challenge in Georgia. Whilst there may be isolated local responses, there is little common understanding or coherent responses to online bullying.
- The scope and availability of illegal child abuse content in Georgia should be thoroughly investigated and actions to prevent access should be taken.

Despite these challenges, Georgia is not without child online protection actions. These activities and efforts are constructive however incoherent and uncoordinated.

Key recommendations

Set up a national stakeholder council, chaired by the government body responsible for ICT policy (The Ministry of Economy and Sustainable Development of Georgia).

Establish and maintain a national centre for removal of illegal child abuse content, which will work jointly with the National Stakeholder Council to develop new strategies and tools to prevent access to child sexual exploitation material.

Create and deliver a national awareness campaign to raise awareness about child online protection issues as well as to make the general public aware of the existence of the National Centre for Child Online Protection and National Stakeholder Council.

Develop and provide professional development programmes for all professionals working with children such as teachers, police officers, and health professionals. A nationwide solution will enable all schools to assess and audit their own child online protection provision against a set of standards and best practice.

Draft, develop and implement a national child online protection strategy to set out the goals and direction that all further actions will be based.

Draft, develop and implement an action plan with activities working towards the goals set out, and covering the issues and topics addressed, in this report as well as to maintain and further improve international cooperation with relevant organisations in the field of child online protection.

Develop a strategy that specifically includes aspects of online bullying as part of the new harassment legislation being developed.

Adapt relevant international, regional and country level resources and further produce national educational resources and reporting mechanisms with regards to online harm and risks.

1 Background and objectives

In line with Resolution 179 (Rev. Dubai 2018) from the Plenipotentiary Conference of the International Telecommunication Union (Busan, 2014[1]) and within the framework of the ITU regional initiative in Europe (WTDC-17, Buenos Aires)[2] on enhancing trust and confidence in the use of information and communication technologies that aims to *support the deployment of resilient infrastructure and secure services allowing all citizens, especially children, to use ICTs in their daily lives with confidence*, a request for ITU assistance was received from the Government of Georgia to address the following:

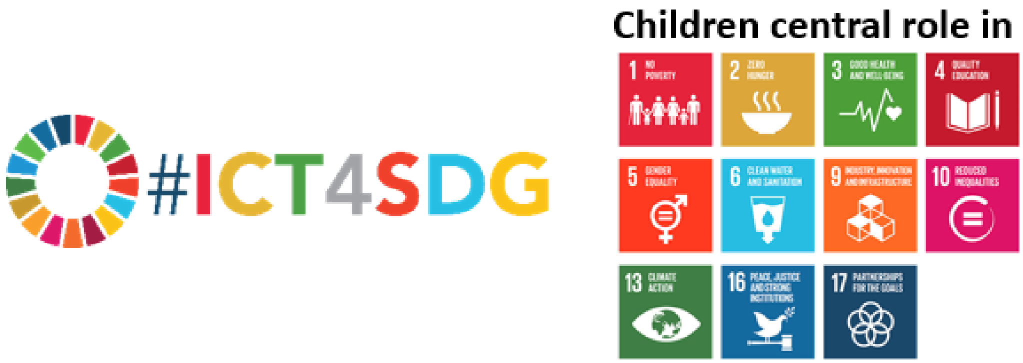
- to assess the existing situation, supplemented by existing statistical sources, covering infrastructure, education, organizational activities and child protection legislation, including identifying gaps in legislation;
- to summarize issues with actual online safety provisions together with any specific recommendations;
- to consider the need for a national online safety strategy and action plan.

The national online safety strategy would encompass governmental entities, information society (young generation, parents, schools, and teachers), telecommunication operators, and the media.

1.1 Sustainable Development Goals

Protecting children is a common thread within 11 of the 17 Sustainable Development Goals. UNICEF puts children at the centre of the 2030 agenda as depicted in Figure 1.

Figure 1: Children, ICTs and SDGs


#ICT4SDG
Children central role in
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
13 CLIMATE ACTION
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

ICTs have been recognized as a key enabler to attain the SDGs. Proper usage of ICTs improve access to basic services like education and healthcare, creates jobs, and empowers communities. More specifically cybersecurity is enshrined in SDG 9 on Industry, Innovation and Infrastructure with the goal *to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.*

Digital natives need to be equipped to make innovative yet safe usage of ICTs.

1.2 Methodology

The report was compiled following preparatory desktop research and supplemented by online surveys completed by children, parents, and stakeholders. Detailed interview meetings were held with a range

[1] https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20179.pdf
[2] https://www.itu.int/md/S16-SG-CIR-0037/en

of government ministries, non-governmental organizations (NGOs), industry, and schools during a mission in October 2018.

The report reflects advice, guidance and recommendations offered in the ITU Guidelines for Policy Makers on Child Online Protection[3]. Within each section, the current situation is explained and issues are identified. The final section illustrates a combined analysis of the situation and details the concluding recommendations. The recommendations are elaborated in terms of priority and timescale together with suggested examples of good practice.

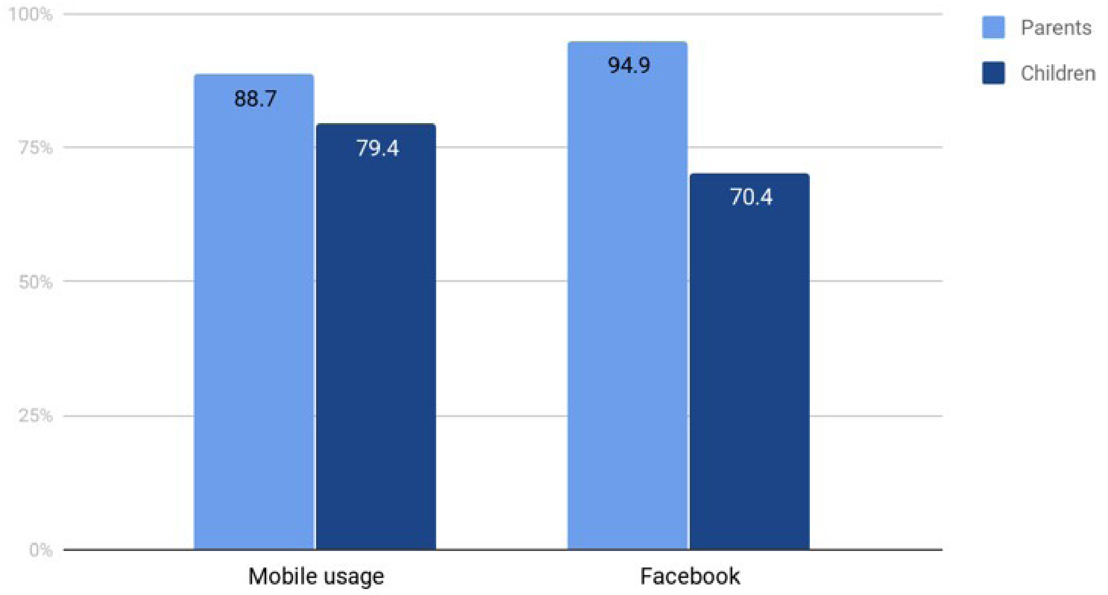
2 Technology and child online protection

Georgia has a growing Internet landscape. ITU concluded that in 2017:

- 60.49 per cent (2.37 million) of the population in 2017 (3.91 million) where using the Internet[4];
- there were 5 730 625 mobile phone subscriptions, representing 146 subscriptions per 100 people[5].

In January 2018, Hootsuite concluded that 2.6 million were actively using Facebook and that this had increased by 18 per cent over the previous 12 months to January 2018.

Figure 2: Mobile and Facebook usage



This data corresponded with the responses to the preparatory online surveys received from 1 154 children and 1 054 parents ahead of the mission. In summary, findings of the preparatory online surveys suggested that in Georgia mobile devices were the primary means used to connect to the Internet (88.7% of parents and 79.4% of children). Interestingly, children were more likely to use a laptop or netbook (33%) compared to parents (15.1%). In terms of extent of use, all parents said they were online for at least an hour a day, compared with 75.8 per cent of children. Having said this, children (possibly older children) were connected for longer (29.6% connected for more than three hours per day) than parents (17.5% connected for more than four hours per day).

[3] https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

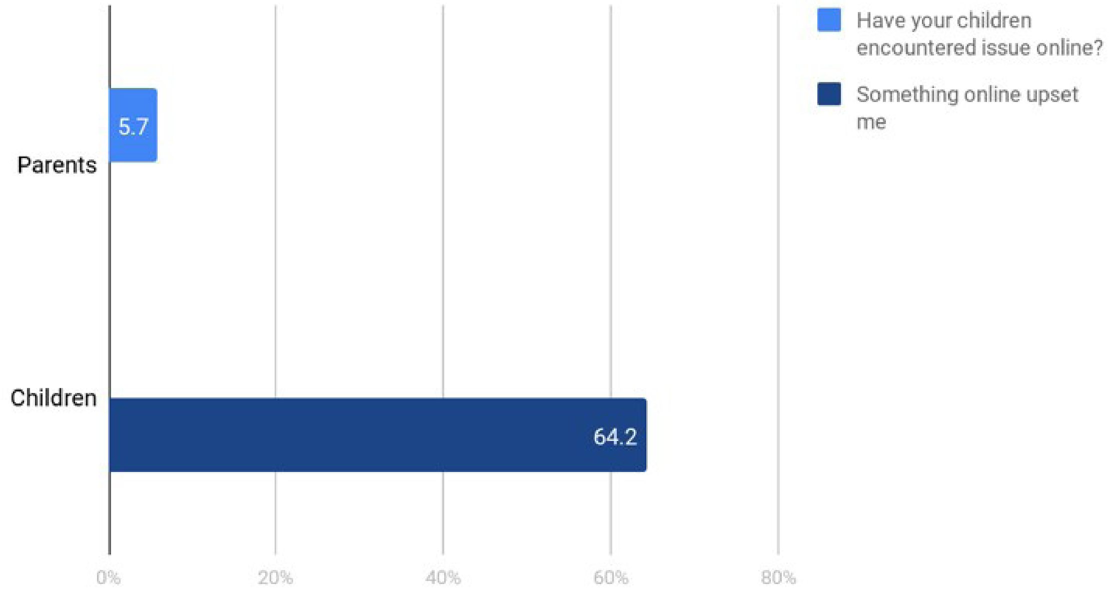
[4] https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/Individuals_Internet_2000-2017.xls

[5] https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/Mobile_cellular_2000-2017.xls

Facebook is the primary social media service used by both children (71.1%) and parents (94.9%), although YouTube is significantly popular amongst children (70.4%).

In terms of online issues, children are most worried by the amount of time they spend online (57.3%), followed by the accuracy of online information (51.8%).

Figure 3: Encountering issues online



Encouragingly, children appear to have confidence in their parents, as most children (67.1%) would talk to their parents about their online concerns. Whilst this is positive, the confidence may be somewhat misplaced as only 5.7 per cent of parents reported that their child had encountered an issue online, compared to 64.2 per cent of children who reported that something online had upset them. Coupled with this, the majority (85.6%) of parents suggest that they do not know how or to whom to report an online issue.

Whilst the online surveys are significant due to the considerable number of responses, the conclusions are for illustrative purposes only. The complete responses can be found in Appendix A (Children) and Appendix B (Parents).

Issues identified

As is common across the world, children in Georgia are significant users and beneficiaries of technology and online services. As highlighted by research (for example EU Kids Online 2011[6]), opportunities created by technology have associated risks, threats, and harm. The surveys, feedback and interviews also identified issues that children are concerned with. Responses from adults, highlighted one prominent concern, the *Blue Whale challenge*. Most of the stakeholders raised questions about this issue during the interviews. Some other examples of cases with online abuse were disclosed, which resulted in the suicide of a child after online extortion and bullying. Reports on these incidents were covered in the Georgia media[7].

[6] http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

[7] https://www.interpressnews.ge/ka/article/508410-arasrulclovani-gogonas-tvitmkvlelobamde-miqvanis-braldebit-ozurgetshi-erti-piri-daakaves/

3 Legal framework

In reviewing the extent to which online safety issues are included within national legislation, the Global Resource and Information Directory (GRID[8]) provided a helpful starting reference of relevant laws within Georgia in 2014. A project of the Family Online Safety Institute and in partnership with UNICEF and the Global WeProtect Alliance, GRID primarily focuses on the "country's laws as they relate to sexual offenses, children and the use of the Internet in the commission of criminal activity". Since amendments to the Georgia Criminal Code in 2010, new offences were introduced affecting child abuse images as well as other cybercrime issues. Specific articles exist in the Georgia criminal code that cover sexual offences in connection to children:

- Article 137, Criminal Code. Rape
- Article 138, Criminal Code. Sexual Abuse Under Violence
- Article 139, Criminal Code. Coercion into Sexual Intercourse or Other Sexual Acts
- Article 140, Criminal Code. Sexual Intercourse or Other Sexual Acts with Children under Sixteen
- Article 141, Criminal Code. Depraved Behaviour
- Article 143.2, Criminal Code. Trafficking of Underage Persons
- Article 171, Criminal Code. Involving a Minor in Antisocial Activity

In the context of child sexual abuse material (often referred to as 'child pornography'[9]), the following articles are most relevant:

- Article 255, Criminal Code. Illegal Production and Trade of Pornographic Materials or Other Items.

This article highlights what pornographic content is considered illegal in context of children and specifically "video or audio material depicting a child's participation in real or simulated sexual scenes, using the voice of a child or demonstrating his/her genitals for the purpose of the sexual satisfaction of another person". In terms of potential sentencing, "an aggravated penalty of correctional work or imprisonment for up to three years, or a fine, will apply for anyone who produces or stores pornographic material containing images of children, or who proposes, transfers, disseminates, sells, advertises or makes available through any other means such material".

- Article 255.1, Criminal Code. Involvement of a Minor in the Illegal Production or Dissemination of Pornographic Materials.

"Defines the offense of involving a minor in the illegal production, dissemination, advertising or sale of pornographic works" and that "the offense is punishable by imprisonment from two and up to four years".

- Article 255^2, Criminal Code. Offering meeting for the sexual purposes to up to 16 years old person.

If an adult has an actual knowledge that the object is up to 16 years old person and offers her/him a meeting by using of information and communication technologies with the aim of Sexual Intercourse or Other Sexual Acts or creating video or audio material depicting a child's participation in real or simulated sexual scenes and after offering such a meeting takes action to achieve the aim.

Offence for the crime defined in this article is imprisonment for the period from 1 to 3 years.

The Ministry of Internal Affairs, and specifically delegates from the Cybercrime Department with responsibility for investigating cybercrime, confirmed the extent of this legislation. Interpol supplies the cybercrime team with information about online child abuse cases to support investigations, specifically IP addressing. During the interview, the cybercrime team reported that one individual has been investigated under this legislation.

[8] https://fosigrid.org/

[9] http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/child-pornography.aspx

Whilst the legislation appears sufficient with regards to online child abuse content, it was concluded that coverage for online bullying or abuse was lacking. This was confirmed by a number of stakeholders, although the Ministry of Internal Affairs confirmed that new harassment laws were already being drafted and that these would cover elements of online bullying. It is encouraging that, during the interviews, a number of stakeholders reported that they are collaborating in workshops in support of this activity.

Child online protection is connected to data protection legislation and specifically the protection of children's data. The Georgia Office of the Personal Data Protection Inspector confirmed that, in connection with data protection laws, the aim is to emulate European Union (EU) data protection legislation, and whilst the General Data Protection Regulation (GDPR) is not incorporated into law, work is being carried out to implement this.

The importance of protecting children is mentioned several times in the GDPR[10]. The major provision in relation to children is Article 8, which requires parental consent to be obtained for information society services offered directly to a child under the age of 16 – although this can be set as low as 13 by EU Member States, and only applies where the processing would be based on the child's consent.[11] [12]

Issues identified

There is no specific legislation that covers online bullying, although work is underway to introduce new laws covering harassment. A common understanding and definition of bullying is needed.

Alignment with GDPR regulations is anticipated and will have an impact on child online protection. According to the GDPR, children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, safeguards, concerns and their rights in relation to the processing of personal data.

Article 8 of the GDPR "Conditions applicable to child's consent in relation to information society services" is highly important.

Recommendation: Legislative framework

The creation of the new harassment legislation should include aspects of child online protection, specifically aspects of online bullying.

Examples of best practice include the 'Enhancing Online Safety Act 2015' in Australia, which establishes a complaints service for children who experience serious cyberbullying.[13]

4 National focus on child online protection

4.1 Stakeholder engagement

Child online protection is of concern to governments, educators, industry and policymakers, and is clearly everyone's responsibility, and is an issue that reaches far outside the borders of just one country. Internet provides wonderful opportunities for children and young people to communicate, share, connect, learn, and access information as well as express their opinions and observations, but this opportunity also presents problems to children's safety, online and offline. As highlighted in many publications and reports by ITU, many national governments have seen the benefit of leading a coordinated child online protection strategy by bringing together all stakeholders and actors to

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[11] https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/24--guide-to-the-gdpr--children.pdf?la=en

[12] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/

[13] https://www.esafety.gov.au/about-the-office/legislation

harness their involvement and to extend collaboration. In terms of opportunities for collaboration, there are some isolated examples of specific activities in Georgia - namely between the ministries of education and internal affairs - in providing school resource officers and the public private cybersecurity forum established by the data exchange agency. However, there is little evidence of a national coordinated approach for child online protection. Engaging all stakeholders is central to the future success of a national child online protection strategy and should include all stakeholders, but specifically representation from:

- government ministries;
- law enforcement;
- industry (telecommunications, technology and service providers);
- non-governmental organizations;
- parents;
- children;
- international organisations;
- academia.

As the governmental body responsible for ICT policy, the Ministry of Economy and Sustainable Development of Georgia hosted the mission and have an excellent understanding and responsibility for child online protection issues. Each of the interview meetings typically overran as a result of the conversations, questions and discussions, evidence of stakeholder appetite to engage in this area. This is further evidenced by a healthy engagement from stakeholders with the national Internet Governance Forum[14] movement. This stakeholder engagement is a strength because the cooperation and participation of all stakeholders is the only reliable way of ensuring successful development and implementation in increasing the level of security and general protection of children online.

Issues identified

There is an appetite and willingness from stakeholders to participate and collaborate on online child protection, albeit in isolation, as there is a need for greater national coordination. Child online protection is clearly a collective responsibility, however, strong orchestration is required to harmonise efforts to amplify and avoid duplication and confusion. It is important to state clearly that children and their experiences and perceptions are carefully considered and integrated into any national collaboration.

4.2 National schools focus

As concluded by Professor Sonia Livingstone in the EU Kids Online final report in 2011[15]:

"*Schools are best placed to teach children the digital and critical literacy skills required to maximise opportunities and minimise risks.* ***Schools are also best placed to reach all children****, irrespective of socioeconomic status and other forms of inequality. For both these reasons, schools have a key role to play in encouraging and supporting creative, critical and safe uses of the internet, crucially throughout the curriculum but also at home or elsewhere*".

UNICEF also concluded in 2017 (Children in a Digital World[16] report) that schools should "Teach digital literacy to keep children informed, engaged and safe online."

[14] http://geoigf.ge/

[15] http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

[16] https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

In establishing a clear view of how schools consider, and to what extent, they protect children online, a significant number of responses to the online stakeholder survey was received and this was supported with interviews with both the Ministry of Education together with representative public and private schools.

It is clear that school responsibility for children extends to online activities, for example, the following two statements are typical of comments received via the online survey "Online safety of children is protected at school" and "We are responsible for online safety and children's rights. The ability for young students to use online tools effectively and safely provides both a skill for life and the means to acquire new skills".

This sense of responsibility for child safety was also articulated by the Ministry for Education. From a national perspective, every school has a Resource Officer, provided and supported by the Ministry of Internal Affairs, who has responsibility for child protection.

In terms of technical security, the Ministry of Education connects all schools to the Internet and provides centralised filtering via Checkpoint[17]. This filtering system is a single, universal list for all users (children and staff) and updated daily from Checkpoint. The Ministry of Education has a filtering policy but this is not published online. The policy includes pornography, gambling, unlicensed software download sites and some messaging services.

Schools are obliged to follow the national curriculum in terms of what is taught and how it is taught, however it is unclear if children receive tuition on protecting themselves to be safer online. Reviewing the responses from schools to the online survey, the emphasis appears to rely on technical security measures to protect children online, for example, the question *How is online safety integrated into your policies?* generated the following response "*Children can't open all the sites that may contain danger for them. The sites are blocked from the Ministry of Education*".

Issues identified

Schools are facing child online protection issues and whilst there is a sense of responsibility, the responses and prioritisation appears inconsistent. Many schools are struggling to recognise and respond effectively to child online protection issues. Although teachers have a variety of capabilities, there is a strong need for help and support in terms of effective practice including increased professional development programmes for staff, reporting routines, curriculum programmes, educational resources, and policy implementation.

The Ministry of Education provides schools with filtered Internet connectivity to block access to specific undesired content. This filtering is universal with no regard to children, adults or age. A filtering policy exists but is not published.

Schools appear not to have a common understanding or expectation about what constitutes suitable and effective child online protection provision. *360 degree safe,* created by SWGfL is a self-review tool that enables schools to assess their own child online protection provision against a set of defined standards and offers individual development plans. The system was since adapted for use in the United Arab Emirates and awarded the WSIS Prize[18] in 2017.

4.3 Cybersecurity

Much work has been successfully undertaken with regards to cybersecurity in recent years, with support from ITU, to produce the Georgia Cyber Security Strategy led by the recently established Data Exchange Agency (DEA). Whilst cybersecurity and child online protection differ, there is overlap in terms of digital skills, online abuse, stakeholder engagement and the reporting of issues.

[17] https://www.checkpoint.com

[18] https://www.itu.int/net4/wsis/prizes/2017/

DEA is an agency within the Ministry of Justice and established to lead cybersecurity. DEA operates the Georgia CERT, handling cybersecurity incidents, Internet traffic, malware, and distributed denial of service attacks (DDOS), and have invested significant efforts in awareness raising, education, and training. For example, DEA developed and implemented a cyber-hygiene training programme for school children, which also covered bullying, however this is not currently mandated. Additionally, DEA have created online training courses on a range of cybersecurity subjects for public servants. DEA has created a public private cybersecurity forum that is working with telecommunication and industry providers to increase online security and resilience.

4.4 Health

Feedback from the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia suggested that the child online protection role is limited to anti-bullying and supporting vulnerable and looked-after children. The ministry recently undertook an awareness campaign of online safety targeting vulnerable and looked-after children. The department for health provides mental health services for teenagers (not specifically Internet-related), and some schools employ psychologists.

Issues identified

The health sector lacks a consistent response to health issues caused by online activities either in connection with child online protection or wider wellbeing issues.

4.5 Data protection

The State Inspector Office (responsible for personal data protection) is an independent legal body overseeing personal data processing by companies and public organisations. The Office accepts reports from the public, removing content where appropriate, and has the power to fine where data protection laws are infringed. In addition, the it provides information and resources about the processing of child data and raises awareness of privacy and data protection-related issues in schools.

Whilst the media is self-regulated in Georgia, the Office has developed and published a code of conduct together with a charter of journalism ethics.

Recommendation: National stakeholder committee

Once established, and chaired by the governmental body responsible for ICT policy (the Ministry of Economy and Sustainable Development of Georgia), a stakeholder committee, supported by a secretariat and composed of stakeholders, should be responsible for establishing a national strategy and implementing an action plan. Examples of best practice include the Council for Internet Safety (UKCCIS) in the United Kingdom.[19]

[19] https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Recommendation: Professional development programmes (teachers, police officers, and health professionals)

To establish a comprehensive professional development programme targeted at those working with children to equip them with an understanding of the risks and harms online as well as the vulnerabilities of children. An example being Online Safety Live[20] in the United Kingdom.

Develop online safety standards for Georgia schools, including classroom resources (e.g. 360 degree safe[21]) that enable schools to assess and audit their own child online protection provision against a set of standards and expectations.

Recommendation: Professional development programmes (teachers, police officers, and health professionals)

It is recommended to establish a comprehensive professional development programme for those working with children. This will help them to understand Internet-related risks as well as the vulnerabilities of children.

A nationwide solution will enable all schools to assess and audit their own child online protection provision against a set of standards and expectations in Georgia. Adapting *360 degree safe*[22] should be considered.

The example set by *Online Safety Live* (UK Safer Internet Centre), which is a programme of free e-safety events for professionals working with children and young people, includes many sector professionals, such as teachers and wider school staff, police officers, health and social workers, adoption and foster professionals, youth workers, local authority, safeguarding professionals. [23]

5 Development of local resources

Georgia has only a limited number of online safety educational resources, including the Office of the Personal Data Protection Inspector 'Alphabet of Online Safety', established in collaboration with the Council of Europe and other EU Member State data regulators.

There is a wealth of effective and valuable online safety resources produced across the world, however adaption for local legislation, culture, context and language is vital. As an example, *360 degree safe*[24], initially designed and developed for schools in the United Kingdom, was only implemented in the United Arab Emirates as the eSafe School programme after careful adaptation, translation, and piloting. ITU recognised the programme with a WSIS[25] award in 2017.

Issues identified

Whilst there are many child online protection tools and resources produced across the world, there is a significant lack of these adapted and translated for Georgia. The relevance and availability of tools and resources tackling child online protection and child safety online is vital not only to enable children, parents, and professionals to be better protected online, but to also articulate its national importance and relevance.

[20] https://www.saferinternet.org.uk/training-events/online-safety-live-free-e-safety-events

[21] https://360safe.org.uk/

[22] https://360safe.org.uk/

[23] https://www.saferinternet.org.uk/training-events/online-safety-live-free-e-safety-events

[24] https://360safe.org.uk/

[25] https://www.itu.int/net4/wsis/prizes/2017/

Stakeholder expectations are low and provision of child online protection in schools across the country needs to be improved. An adaptation of the 360 degree safe programme (e.g., the eSafe school programme in the United Arab Emirates) may be suitable for Georgia to empower every school to appreciate their current online safety provision but more importantly be supported to generate a development plan that will ensure every school has a consistent and at least an essential level of child online protection provision.

Recommendation: International cooperation and action plan

Following the publication of a national child online protection strategy, the next task for a national committee for child online protection should be to draft and publish an action plan. An example of best practice and strategic vision was issued by the Welsh Government[26] in 2018.

Child online protection challenges are borderless, spilling over from one country to another, making international cooperation essential. Government and stakeholders should continue to work with international partners to identify examples of best practice to implement the action plan. Examples of international cooperation and resource adaptation can be found in INHOPE[27] and INSAFE[28] networks and the COP[29] website.

6 Public education and awareness

It is clear from the feedback of the preparatory research coupled with stakeholder interviews that low public awareness and understanding of online risks and threats remains a major challenge. This issue was consistently commented on by stakeholders, who also repeatedly noted the need to make raising awareness a priority. Evidence from the preparatory online survey indicates that only 5.7 per cent of parents reported that their child had encountered an issue online, and yet, 64.2 per cent of children reported that something online had upset them. Coupled with this, the majority of parents (85.6%) suggest that they do not know to whom or how to report an online issue.

Awareness raising programmes are typically multi-dimensional, targeting parents as well as those working with children. Signposting resources, self-help, and supplementary professional development training programmes, would benefit those working with children (such as teachers), given their elevated responsibilities.

The Georgian National Communication Commission (GNCC) has responsibility for media literacy since 2018 and has built a four pillar programme with support from by the Bavaria Media Regulator, including:

- media school: to provide training for journalists to improve skills;
- media laboratories: to highlight digital journalism and new technologies to support media;
- media criticism: to improve critical evaluation skills in connection with the spread of fake news;
- awareness raising programmes: to improve media literacy amongst parents, children and teachers.

The GNCC intends to undertake research across the country to highlight media use, consumption, and access.

[26] https://gov.wales/sites/default/files/publications/2018-07/online-safety-action-plan-for-children-and-young-people-in-wales.pdf

[27] http://www.inhope.org/gns/home.aspx

[28] https://www.betterinternetforkids.eu/

[29] https://www.itu.int/en/cop/Pages/default.aspx

Guidelines for policy makers on child online protection

When producing educational materials, it is important to bear in mind that many people who are new to the technology will not feel comfortable using it. For that reason, it is important to ensure that safety materials are made available in either written form or produced using other media with which newcomers will feel more familiar, for example, with video.

*Within any education and awareness campaign it will be important to strike the right tone. Fear-based messaging should be avoided and due prominence should be given to the new technology's many positive and fun features. The Internet has great potential as a means of empowering children and young people to discover new worlds. Teaching positive and responsible forms of online behaviour is a key objective of education and awareness programmes.**

* ITU Guidelines for policy makers on child online protection
https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

The Ministry of Economy and Sustainable Development of Georgia and the Internet Society both highlighted their collaborative plans to build a Safer Internet Day[30] campaign. Now in its fifteenth year, Safer Internet Day is celebrated across 140 countries and an ideal platform to construct and launch a significant campaign that will create a long-term national discussion.

Issues identified

The general awareness of child online protection across Georgia is weak. This was universally identified by stakeholders, disclosed in the online surveys. Educating the public about the online challenges and threats as well as pointing to the positive side of the Internet is missing and should be at the heart of such awareness activities as well as giving information about what, where, and how to report in the event of encountering such issues online.

Recommendation: National awareness campaign

Raising awareness about child online protection issues amongst the general population is of vital importance. Effective awareness-raising campaigns can be found in the example of Safer Internet Day celebrations in the United Kingdom Safer Internet Centre.

Safer Internet Day 2018 was celebrated globally on Tuesday 6 February 2018 with the slogan *Create, Connect and Share Respect: A better internet starts with you.* [31]

7 Reporting mechanisms and tools

For the purposes of this report, reporting mechanisms will be divided into:

- illegal child online abuse content;
- harmful and abusive online content, including bullying; and
- use of technical tools

[30] https://www.saferinternetday.org/
[31] https://www.saferinternet.org.uk/safer-internet-day/2018

7.1 Illegal online child abuse content

In terms of illegal content, chapter 3 of ITU guidelines for policy makers on child online protection concerns itself specifically with child abuse material. Whilst the Cybercrime unit, within the Ministry of Internal Affairs appears to have responsibility for investigating offences relating to online child abuse content, it is unclear if the level of resourcing and prioritisation applied to this activity is appropriate and if this is suitable. It appears that the Cybercrime unit is supported by Interpol in this regard, which is encouraging. However, there is little public understanding of what illegal online child abuse content is, which may suggest why the number of investigations is low.

The Georgian National Communication Commission (GNCC) shared their plans to create a national centre for child online protection to monitor and ensure child online safety with a hotline to receive reports from the public regarding illegal child abuse content, and with the power to take down content. This aspect of the centre is being developed with support from the Lithuania hotline and is expected to become a INHOPE[32] member.

It is expected that law enforcement will be engaged in this process to support both the removal of any content hosted in Georgia as well as investigating individuals accessing illegal content. Depending on the scope of the national centre, it is also possible that law enforcement officers will be required to review and validate reported content.

In terms of availability of illegal online child abuse content, currently there are no mechanisms preventing access to this content. Industry, specifically telecommunication operators will play an important role in establishing a robust national response to illegal online child abuse content, specifically in measures to restrict availability of illegal content to users. Existing legislation would require the removal of any reported illegal content found to be hosted within their environments and issued with a takedown notification.

The objective of creating a national centre for child online protection requires wide public, stakeholder and partner engagement and awareness.

Issues identified

Whilst the establishment of a national centre for child online protection to manage online child abuse images is underway by GNCC, there is much work to do. Awareness across stakeholders is lacking and obtaining their understanding, support and participation is vital in ensuring the successful establishment of the national centre. Child abuse images are already covered within the legislation making them illegal and providers hosting this material will be required to comply with any take down notification to remove the offending content. There is currently no obligation for telecommunication providers to restrict access to illegal online child abuse content and they should be encouraged to adopt and deploy mechanisms to do this. This may require legislation if self-regulation is unsuccessful. The national centre for child online protection should be adequately governed with oversight, perhaps by a national stakeholder committee, the Ministry of Internal Affairs, or the Ministry of Economy and Sustainable Development of Georgia. In addition to this, wider public awareness is required to ensure that there is an understanding of where and how to report content.

7.2 Harmful and abusive online content, including bullying

It is clear from both the online survey responses together with stakeholder interview feedback that bullying is a significant concern and challenge. Comments from the Ministry of Education and Ministry of Health highlighted that even a basic and consistent definition of bullying was lacking. There is a gap in legislation with regards to bullying, although work has already been initiated in drafting new harassment laws, which is understood to include bullying, it is expected that the new laws will also be required to establish a common definition of bullying.

[32] https://www.inhope.org

In terms of the extent of bullying incidents, the Children's Rights Centre within the Public Defender (Ombudsman) of Georgia responsible for protecting children's rights shared a recent report that included a section on bullying, which stated that:

The results of the monitoring made it clear that the protection of children from abusive approach and improper treatment remains a challenge in the system of general education: psychological and physical abuse of children by adults and peers is observed frequently; bullying among pupils is a widespread form of interaction among minors; awareness of pupils of their rights is poor; responsible persons lack competence regarding the mechanism of response to all forms of violence against children and hence, response is not undertaken in the best interests of the child; there is a shortage of psycho-social rehabilitation services for child victims.[33]

It is worthy of note that, as the media regulator, the GNCC is receiving reports relating to harmful online content and referring these to the provider (typically social media provider) to take down harmful and/or abusive content. During the discussions, it is assumed that no organisation has 'trusted flagger' status (or similar); the elevated standing given to organisations, recognising their understanding of the reporting policy and process and often fast tracking or prioritising the submitted reports to social media providers. It may be helpful for any organisation with a public facing reporting function within Georgia to seek this status with relevant providers.

Recommendation: National centre to manage and remove illegal child abuse content

Establishment of a national centre to manage and remove illegal child abuse content is crucial and should be carried out as soon as possible.

Examples of centres is the IWF[34] in the United Kingdom (run by an NGO), and Draugiskas Internetas[35] by the media regulator in Lithuania[36].

Recommendation: Online harm

It is clear that action and support to combat all forms of bullying, but particularly in the context of online bullying, is required. It is expected that the new legislation will greatly help, however further updates to policy, professional development, curriculum and educational resources is required. In the long term, a mechanism to report harmful digital content would safeguard children. An example exists in Australia, provided by the Office of the eSafey Commission[37] with powers under the Enhancing Online Safe Act in 2015.

[33] Special Report: VIOLENCE AGAINST CHILDREN IN GENERAL EDUCATIONAL INSTITUTIONS

[34] https://www.iwf.org.uk/

[35] https://pranesk.draugiskas/

[36] https://pranesk.draugiskasinternetas.lt/

[37] https://www.esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying

The Blue Whale challenge

Most stakeholders raised questions following reports on the so called ‘Blue Whale’ challenge, reportedly responsible for a number of teenage deaths in Russia. However, the Georgian Cybercrime unit, within the Ministry of Internal Affairs, confirmed that it has been actively investigating this phenomenon, and in addition to reports from online fact checking websites, they reported that although there have been reports of young people committing suicide in Russia over the last six months, of these reported cases none have been found to have had a conclusive evidence of links to the 'Blue Whale' challenge.

Participation in online challenges and competition with other children will always been a concern, as unfortunately, some challenges are directed at risky and dangerous behaviour for children and young people. The readiness of a child to engage in inappropriate or potentially dangerous activities through any form of technology depends on a number of factors such as the influence of friends, the media, the level of self-confidence, the quality of relationships and trust among family members or in the neighbourhood, parental control.

All evidence indicates the need for parents, carers, and children to have open and honest conversations about what they are seeing online, talking through some of the issues that this game has brought to light, such as self-harm and negative influences online, and underlines the need to teach children and young people to recognize what is harmful to them, and to create a safe environment in which they can safely use and benefit from the online experience.

New challenges or games are a part of the innovative element of the Internet, parents and children need to know about the potential for online harm, and children need to have the confidence to speak to their parents about what they are doing online.

7.3 Use of technical tools

The general level of awareness of online risks and threats is low, particularly amongst parents. This is at a time when the number of connected devices and technologies within households and families is increasing.

Parental responses to the question ‘Do you use any filtering or monitoring software on any of your children’s devices?’ suggested that whilst 15.5 per cent do, the majority (53.3%) do not. More significantly, a large number (31.2%) indicated they would like to, but don’t know how to set it up. In discussions with operators, and contrary to expectations, it emerged that they provide no form of filtering or blocking technologies for their customers.

Operators offer customers some support via call centres, particularly in relation to telephone fraud, although the call handlers receive no formal training and so responses will vary. Additionally, there are typically no staff with recognised knowledge to support call handlers with particular customer queries.

Operators expressed a desire to publish recommendations on their website to support customers, especially security information, for example, advice on passwords, phishing etc.

Whilst operators generally articulated resistance to network-wide filtering, there was an understanding of developing and implementing technology tools in context of restricting access to illegal child abuse content such as tools to support parents in filtering / blocking technologies to reduce the exposure to inappropriate content. Help and support to implement this type of technology would be required, especially to companies that have already implemented such technology with a view to sharing best practice, in addition to internal commercial discussions before any commitment could be made.

Industry can identify, prevent, and mitigate the adverse impacts of ICTs on children's rights, and opportunities to support the advancement of children's rights, by integrating them into corporate policies and management processes[38]. In collaboration with government, law enforcement, civil society and hotline organisations, industry has a key role to play in combating child sexual abuse material with developing standard processes to handle such material. Industry can help create a safer, more enjoyable digital environment for children of all ages by creating a safer and age appropriate online environment. Industry can complement technical measures with educational and empowerment activities aimed at educating children, parents, and teachers about children's safety and their responsible use of ICTs. Industry can encourage and empower children by supporting their right to participation by promoting digital technology as a way to further civic engagement.

Issues identified

In addition to the challenges in communicating the perils of harmful content to parents, and adults in general, there is a lack of locally created technical tools to enable them to protect children. The lack of skills, support, and cooperation needed to build and disseminate these tools is a major issue.

Recommendation: Create parental control tool policy and strategy

This is not an easy task. At the end of 2018, the European Union published recommendations and the results of a survey as a continuation of the UN Safer Internet Action Plan. However, the benchmarking exercise of parental control tools for the online protection of children suggests that "… most parental control tools fail to sufficiently address the needs of the parents to protect children against online risks."[39]

Despite the struggle, it is recommended to create the necessary policy and strategy that will boost safe use of the Internet by young people, such as the online safety action plan for children and young people that was published by the Government of Wales[40].

8 Analysis and recommendations

8.1 SWOT analysis

In assessing the evidence, comments and feedback, the following strengths, weaknesses, opportunities, and threats were determined in further support of the recommendations.

[38] ITU guidelines for industry on COP: https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf

[39] https://ec.europa.eu/digital-single-market/en/news/benchmarking-parental-control-tools-online-protection-children

[40] https://gov.wales/sites/default/files/publications/2018-07/online-safety-action-plan-for-children-and-young-people-in-wales.pdf

Table 1: SWOT Analysis

Strengths	**Weaknesses**
• Wide variety of stakeholders. • Existing collaborative structures, including National IGF. • Willingness to improve on the field of child online protection. • Understanding the complexity and need for cooperation. • Georgia is in the top 6 countries in the world regarding cybersafety. • NGO involvement in the area of online child safety.	• Lack of national strategy and coordination. • Lack of awareness of child online protection and safety related threats and risks. • Lack of published standards or expectations for organisations and agencies working with children. • Lack of child online protection tools and resources, particularly those adapted for Georgia.
Opportunities	**Threats**
• Wide variety of stakeholders interested in the topic. • International support for the adaptation and implementation of activities, tools and resources. • Governmental support for the development and implementation of child online protection. • Using best practice examples from the international community.	• No coordinated systems, actions or activities undertaken. • Children remain vulnerable to online risks. • Research is not undertaken on the issues, leaving *urban myths* (e.g. Blue Whale) to often propagate. • Parents and professionals have no support in education or reporting issues.

8.2 Recommendations

Table 2: Detailed recommendations

1. Set up a national stakeholder committee, chaired by the governmental body responsible for ICT policy, the Ministry of Economy and Sustainable Development of Georgia (MoESD)	
Overview	**Priority / Timescales**
Such a committee should consist of interested stakeholders from ISPs, NGOs, government entities, data regulators, parents and youth/children etc. The committee will govern, debate and offer guidance on this topic. The committee may determine that sub-working groups be created to undertake specific activities. Given the ministry responsibilities for national ICT policy, the committee should be chaired by the MoESD. The capability, capacity and existing responsibilities of MoESD make them ideal to chair the committee. Meetings should be organised at a suitable frequency. The committee should be supported by a MoESD secretariat to organise and manage the meetings logistics (venue, issue papers, minutes, logistics). The committee should initially be tasked with drafting a national child online protection strategy and action plan.	Priority – 1 To establish the committee and hold the inaugural meeting within 6 months. The Child Online Protection Strategy to be published within 12 months. The Child Online Protection Action Plan to be published within 18 months.
Examples UK Council for Internet Safety- https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis Guidelines for Policy Makers on Child Online Protection, United Nations ITU, https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf	

2. Establish a national centre for child online protection to manage and remove illegal child abuse content	
Overview	**Priority / Timescales**
The establishment of a national centre for child online protection should have the following characteristics. • Assess content – the capability to assess and grade online child abuse content in line with legislation. It is important to ensure that assessment is in line with legislation. For example, the legislation may dictate that this assessment of illegal child abuse images be conducted by law enforcement and in which case referral procedures required. • Public reporting – to receive reports online child abuse content from the public. • Law enforcement – to liaise with law enforcement with operational referrals and information exchange. • Take down – issue take down notifications for content being hosted within Georgia. Take-down notifications may be issued by either the national centre for child online protection or law enforcement (depending on national requirements), but existing legislation ensures that companies hosting identified illegal content will be required to comply and remove offending content. Support can be provided in both the issuing of take down notifications and take down actions of telecommunication providers. • INHOPE and international cooperation – exchange information on illegal child abuse content. • Availability of illegal child abuse content – It is recommended that the national centre for child online protection work with the national telecommunication providers, initially in a self-regulatory approach, to reduce availability of known online child abuse content. It is clear from the interest from all stakeholders, in particular from industry and telecommunication providers, that there is much interest in child online protection. To restrict access to illegal child abuse content and further re-victimisation of children, it is recommended that telecommunication providers block access to identified illegal child abuse. This recommendation should make a URL list available (automated and secure) to telecommunication providers to deploy within their networks to restrict user access to this content. This URL list will contain the URL addresses of known illegal child abuse content located in any country in the world and is in line with many other examples in Europe. Should self-regulatory approach not be successful, additional legislation and regulation may be required. It is recommended that the national centre should have adequate governance, reporting to a national stakeholder committee and specifically the governmental body responsible for ICT policy, The Ministry of Economy and Sustainable Development of Georgia.	Priority – 1 To have created the national centre for child online protection within 6 months. To have fully completed the establishment of the centre with all agreed functions within 12 months.

Examples

Lithuanian hotline- https://pranesk.draugiskasinternetas.lt/

Internet Watch Foundation- https://www.iwf.org.uk/

3. Create a national child online protection awareness campaign	
Overview	**Priority / Timescales**
Improvements to the general awareness of the population is needed on a national scale. The understanding and appreciation of target audiences (e.g. children, teachers, parents and grandparents) to recognize the risks, issues and threats through a national conversation is clearly important to prevent harm. It is vital that this campaign provides suggested solutions and call to action in terms of combating and resolving the threats and harms. The recommendation is to build an awareness campaign through a national Safer Internet Day campaign. Focusing efforts on a single day will present opportunities for a national discussion and dialogue. With suitable orchestration, a broad range of stakeholders can be engaged to repeat online safety messages to significantly extend reach into the population, especially target audiences. Stakeholders should be engaged on the lead up to Safer Internet Day, being provide with information, content and communications to ease and improve their involvement and impact. There are many examples from across Europe (where Safer Internet Day was created in 2004) of successful Safer Internet Day campaigns and would include social and printed media campaigns, alongside engaging partner stakeholder media channels. Having a coordinated and unified approach is important to ensure that all those involved are repeating the same syndicated messaging. The awareness raising campaign should utilise the research and national data being developed by GNCC to highlight the use and adoption of technology by children and parents across Georgia. The programme should also include an evaluation to measure the impact to enable comparisons with subsequent years to determine progress. Further events and conferences opportunities can be used to further promote these messages, so that the campaign has sustained impact beyond the single day.	Priority – 1 To complete Safer Internet Day 2019 as planned and complete evaluation research to determine reach and impact of activities. To engage a broader set of stakeholders and awareness campaign for Safer Internet Day 2020 and 2021, evaluating reach and impact to monitor progress

Examples

Safer Internet Day
United Kingdom https://www.saferinternet.org.uk/safer-internet-day/2018

Global
https://www.betterinternetforkids.eu/web/sid/home

European Union
https://www.betterinternetforkids.eu/web/portal/practice/awareness

4. Establish a national professional development programme for teachers, police officers, and health workers.	
Overview	**Priority / Timescales**
Those working with children have additional responsibilities in the protecting of children. Their capability to recognise, respond and resolve issues is critical. The development and implementation of a national professional development programme for those working with children, in particular teachers, resource officers, social workers, that provides them the following: • Understanding of the risks and harms online and how children encounter these. • Ability to recognise online issues. • Knowledge of how to respond and escalate issues, using existing processes. • Educational resources and support to educate children to be safer online. This programme should be delivered through both professional training for key staff (Resource Officers and those with specific child protection responsibilities) and supplemented with remote or online content for all other professionals. This programme should be integrated into the existing child protection training programmes and obligations Implementation of the eSafe School Programme to empower schools to self-review their own online safety provision. The programme will adopt a set of national standards for schools to assess their provision, highlighting the strengths and weaknesses and create a development plan to meet the national standards. The data will disclose the performance and progress of national schools.	Priority – 2 To have created a national certified professional development programme within 6 months. Complete a pilot programme reaching 50 professionals and evaluate the feedback over the next 6 months. Extend a national professional development programme. Explore the implementation of eSafe school with support of ITU. Exploration programme within 3 months. National adaptation and drafting of national standards for schools to perform and be measured against. An additional 6 months. System development and publication online.
Examples Australia- https://www.esafety.gov.au/ INSAFE EU- https://www.youtube.com/watch?v=IpbJ-8s2DEE EU- https://www.etwinning.net/en/pub/index.htm Common Sense Media- https://www.commonsensemedia.org/ Guidelines for Educators on Child Online Protection, United Nations ITU, https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf Aqdar eSafe School Programme- https://esafeschool.ae. (This is an adaptation of www.360safe.org.uk)	

5. International cooperation and action plan	
Overview	**Priority / Timescales**
The Georgia Government and stakeholders should continue to work with international partners to identify further examples of best practice to adapt and adopt. A national committee for child online protection should drive the development of existing and new activities and programmes for child online protection; for example: • Resource creators with a view to adopt and adapt for use within Georgia, in particular resources focused on the issues that children are concerned with mostly (potentially screen time and fake news). • Content for professional development programmes. • support industry stakeholders with options to implement age appropriate filtering through international cooperation. • Increase the level of social corporate responsibility in the business sector. The publication of a national action plan integrating examples highlighted in this report (e.g., eSafe school programme), prepared by a national committee for child online protection.	Priority – 1 Organise an expert conference with stakeholders within 6 months. Priority – 2 Connect telecommunication operators and industry to international industry partners to develop safety tools within 6 months.

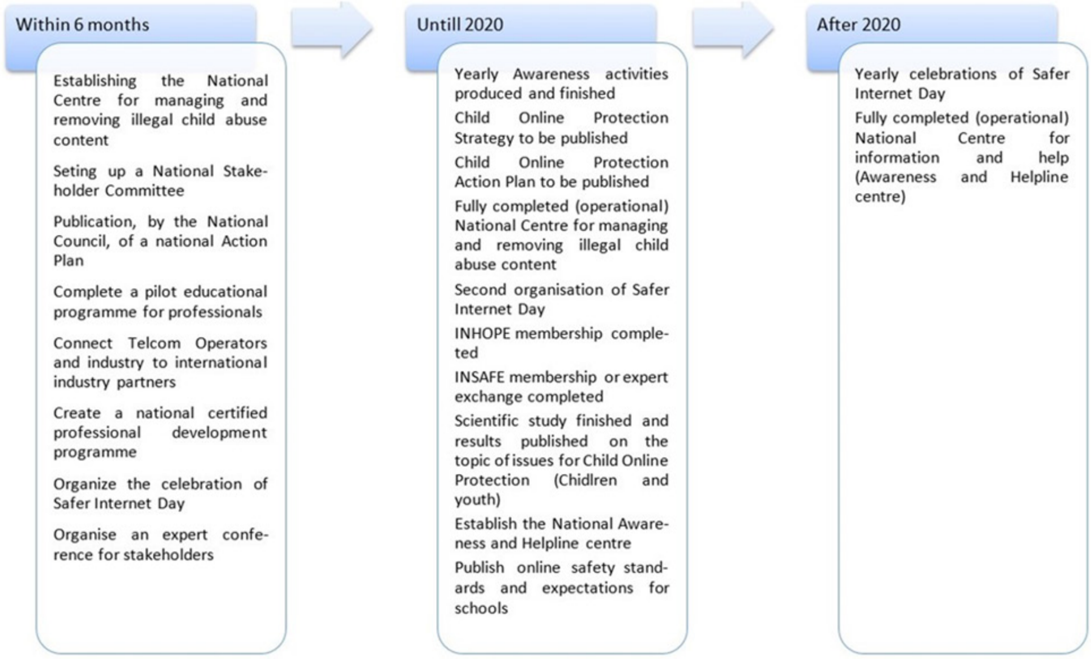
<table>
<tr><th colspan="2">5. International cooperation and action plan</th></tr>
<tr><th>Overview</th><th>Priority / Timescales</th></tr>
<tr><td colspan="2"><b>Examples</b>
Work closely with the COP initiative and share lessons learned at the ITU Council Working Group on Child Online Protection. https://www.itu.int/en/council/cwg-cop/Pages/default.aspx</td></tr>
<tr><th colspan="2">6. Legislation framework to include online bullying in planned harassment legislation</th></tr>
<tr><th>Overview</th><th>Priority / Timescales</th></tr>
<tr><td>The creation of the new harassment legislation should include aspects of child online protection, specifically aspects of online bullying.</td><td>Priority – 2
Complete new harassment legislation within 12 months.</td></tr>
<tr><td colspan="2"><b>Examples</b>
Examples include the ‘Enhancing Online Safety Act 2015’ in Australia that establishes a complaints service for children who experience serious cyberbullying[41]</td></tr>
<tr><th colspan="2">7. Online Harms: Define online harms and produce educational resources and reporting mechanism</th></tr>
<tr><th>Overview</th><th>Priority / Timescales</th></tr>
<tr><td>It is clear that action and support to combat all forms of bullying, but particularly in this context online bullying is required. It is expected that the new legislation will greatly help, however further updates to policy, professional development, curriculum and educational resources is required. Longer term, a mechanism to report harmful digital content would support children facing this issue.</td><td>Priority – 2
Create and publish education resources.
Priority – 3
Create a reporting mechanism and centre.</td></tr>
<tr><td colspan="2"><b>Examples</b>
An example exists in Australia, provided by the Office of the eSafey Commission[42] with powers under the Enhancing Online Safe Act in 2015.</td></tr>
<tr><th colspan="2">8. Create parental control tool policy and strategy</th></tr>
<tr><th>Overview</th><th>Priority / Timescales</th></tr>
<tr><td>This is not an easy task. At the end of 2018, the European Union published recommendations and the results of a survey as a continuation of the UN Safer Internet Action Plan. However, the benchmarking exercise of parental control tools for the online protection of children suggests that “… most parental control tools fail to sufficiently address the needs of the parents to protect children against online risks.”
Despite the struggle, it is recommended to create the necessary policy and strategy that will boost safe use of the Internet by young people, such as the online safety action plan for children and young people that was published by the Government of Wales.</td><td>Priority – 3
The Child Online Protection Strategy to be published within 12 months.
The Child Online Protection Action Plan to be published within 18 months.
Priority – 3
Create a reporting mechanism and parental control tool.</td></tr>
<tr><td colspan="2"><b>Examples</b>
Government of Wales online safety action plan for children and young people.
https://gov.wales/sites/default/files/publications/2018-07/online-safety-action-plan-for-children-and-young-people-in-wales.pdf</td></tr>
</table>

[41] https://www.esafety.gov.au/about-the-office/legislation

[42] https://www.esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying

8.3 Proposed time line

Figure 4: Summary time line



Within 6 months

Establishing the National Centre for managing and removing illegal child abuse content

Seting up a National Stakeholder Committee

Publication, by the National Council, of a national Action Plan

Complete a pilot educational programme for professionals

Connect Telcom Operators and industry to international industry partners

Create a national certified professional development programme

Organize the celebration of Safer Internet Day

Organise an expert conference for stakeholders

Untill 2020

Yearly Awareness activities produced and finished

Child Online Protection Strategy to be published

Child Online Protection Action Plan to be published

Fully completed (operational) National Centre for managing and removing illegal child abuse content

Second organisation of Safer Internet Day

INHOPE membership completed

INSAFE membership or expert exchange completed

Scientific study finished and results published on the topic of issues for Child Online Protection (Chidlren and youth)

Establish the National Awareness and Helpline centre

Publish online safety standards and expectations for schools

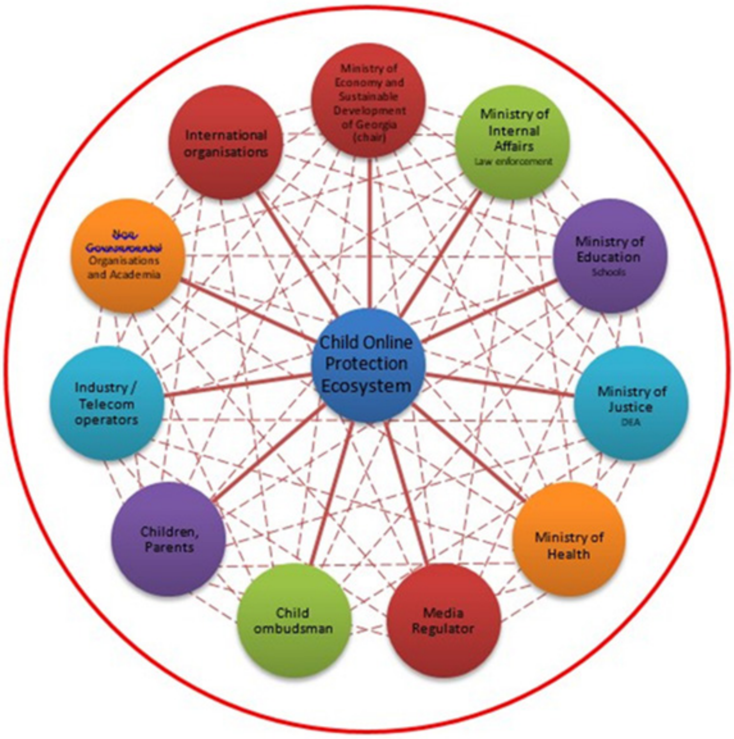
After 2020

Yearly celebrations of Safer Internet Day

Fully completed (operational) National Centre for information and help (Awareness and Helpline centre)

8.4 Child online protection ecosystem in Georgia

Figure 5: National Committee for Child Online Protection composition


Child Online Protection Ecosystem
Ministry of Economy and Sustainable Development of Georgia (chair)
Ministry of Internal Affairs Law enforcement
Ministry of Education Schools
Ministry of Justice DEA
Ministry of Health
Media Regulator
Child ombudsman
Children, Parents
Industry / Telecom operators
Non Governmental Organisations and Academia
International organisations

8.5 Responsibility

Whilst the responsibility for considering these recommendations may be with the Ministry of Economy and Sustainable Development of Georgia, through a national committee for child online protection, the implementation of these recommendations could be the responsibility of a new agency aligned, for example, with the European Union Safer Internet Programme,[43] which may have many benefits in terms of support. In this EU programme, there are 32 national centres, each centre undertaking and implementing similar strategies and activities within their country.

[43] https://www.betterinternetforkids.eu/

References

ITU Guidelines for Policy Makers on Child Online Protection, https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

ITU Guidelines for children on Child Online Protection, https://www.itu.int/en/cop/Documents/guidelines-children-e.pdf

ITU Guidelines for parents, educators and guardians on Child Online Protection, https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

ITU Guidelines for industry on Child Online Protection, https://www.itu.int/en/cop/Documents/guidelines-industry-e.pdf

360 degree safe, SWGfL, https://360safe.org.uk/

Children in a Digital World, UNICEF, 2017, https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

EU Kids Online, Livingstone S (2011), http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20I%20(20069)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

Framework of the ITU Regional Initiative on Europe (WTDC-17, Buenos Aires), https://www.itu.int/md/S16-SG-CIR-0037/en

Georgian Internet Governance Forum, http://geoigf.ge/

GRID (Global Resource and Information Directory), FOSI in partnership with UNICEF and Global WeProtect Alliance 2014, https://www.fosigrid.org/republic-of-georgia

Guide to GDPR – Children, Bird & Bird (2018), https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/24--guide-to-the-gdpr--children.pdf?la=en

Guide to GDPR, ICO, 2017, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/

INHOPE, http://www.inhope.org/gns/home.aspx

INHOPE, Definition of Child Sexual Abuse Material, http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/child-pornography.aspx

INSAFE, https://www.betterinternetforkids.eu/

Inter News Press Article 2018, One person was detained in Ozurgeti for kidnapping a minor to suicide), https://www.interpressnews.ge/ka/article/508410-arasrulclovani-gogonas-tvitmkvlelobamde-miqvanis-braldebit-ozurgetshi-erti-piri-daakaves/

ITU Child Online Protection, https://www.itu.int/en/cop/Pages/default.aspx

ITU Resolution 179, ITU's role in child online protection 2014, https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20179.pdf

National online safety action plan for children and young people, Welsh Government, 2018 https://gov.wales/newsroom/educationandskills/2017/170517-national-online-safety-action-plan-for-children-and-young-people-to-be-created-kirsty-williams/?lang=en

Safer Internet Day Home Page, https://www.saferinternetday.org/

Online Safety Live Professional Development Training Programme, UK Safer Internet Centre, https://www.saferinternet.org.uk/training-events/online-safety-live-free-e-safety-events

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Safer Internet Day (United Kingdom), https://www.saferinternet.org.uk/safer-internet-day/2018

Summary of the Enhancing Online Safety Act 2015 (Australia, Office of the Australian eSafety Commissioner, https://www.esafety.gov.au/about-the-office/legislation

UK Council for Internet Safety, https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

We are Social, Global Digital Report, Hootsuite (2018), https://wearesocial.com/blog/2018/01/global-digital-report-2018

WSIS Prizes 2017, https://www.itu.int/net4/wsis/prizes/2017/

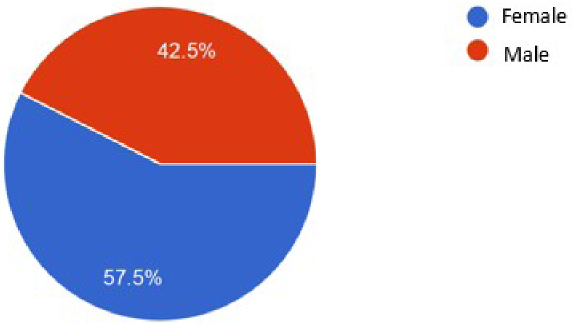
WTIS-18: Impact of telecommunications/ICTs and emerging technologies on social and economic development, ITU statistical data, https://www.itu.int/en/ITU-D/Statistics/Pages/events/wtis2018/default.aspx

- Percentage of Individuals using the Internet, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/Individuals_Internet_2000-2017.xls
- Mobile-cellular subscriptions, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/Mobile_cellular_2000-2017.xls

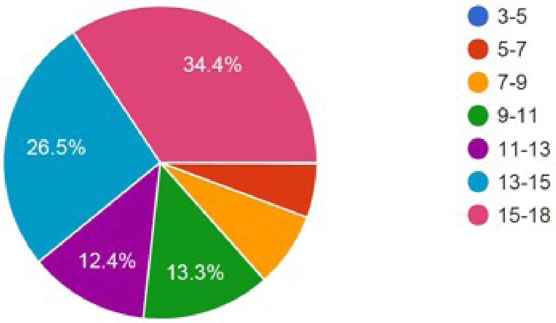
Appendix A: Child online survey results

Children and youth (1,154 Responses)

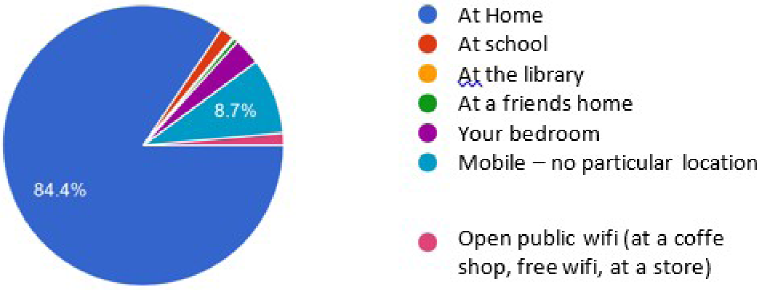
1. Male\Female



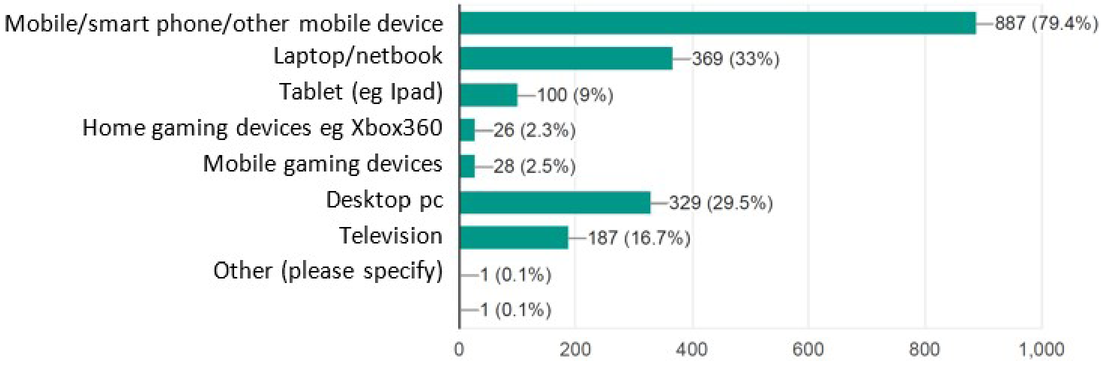
2. How old are you:



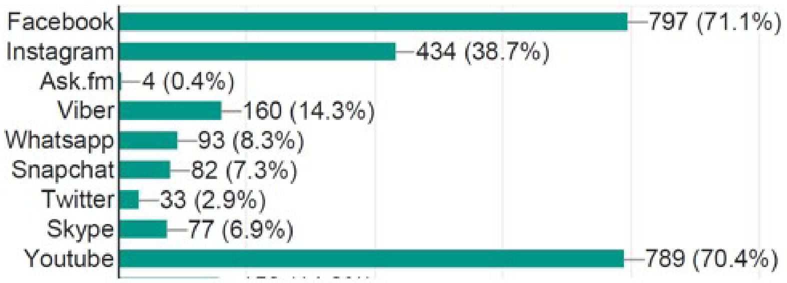
3. Where do you most often connect to the internet?



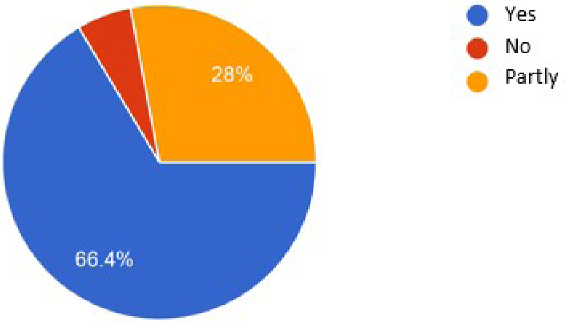
4. What do you use to go online? (please tick all you use)



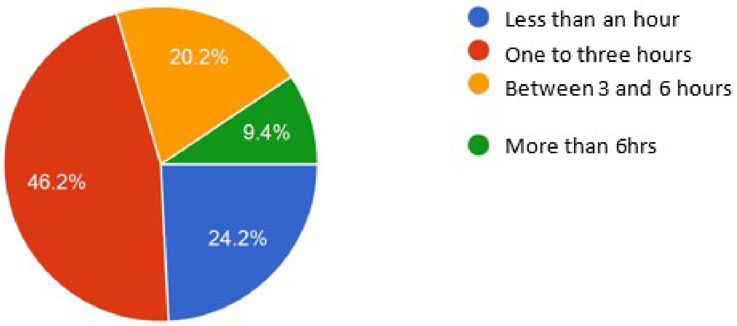
5. What of these social media, do you use most often? (circle multiple answers)



6. Do your parents know what you do online?



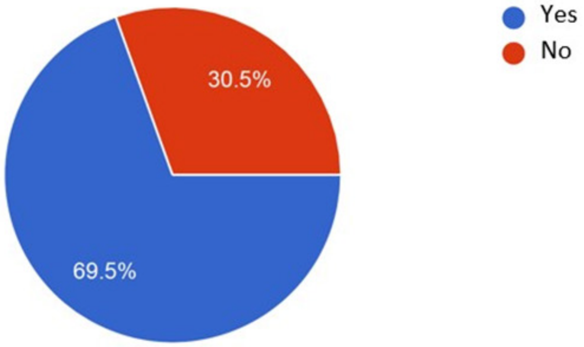
7. How much time do you spend online in an average day?



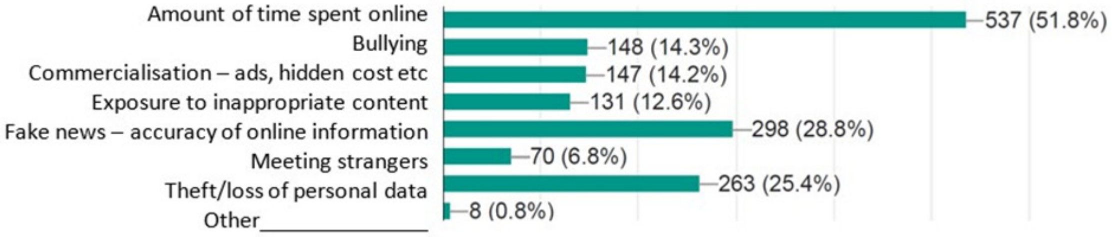
8. What do you use the Internet for?
   - Social networks
   - Instant messaging, eg Windows live, Skype.
   - Gaming
   - Shopping
   - News
   - Browsing/general entertainment
   - Listening to music
   - Uploading/content creation eg Youtube

9. Have you ever met in person with a friend you only met online?
   - Yes
   - No

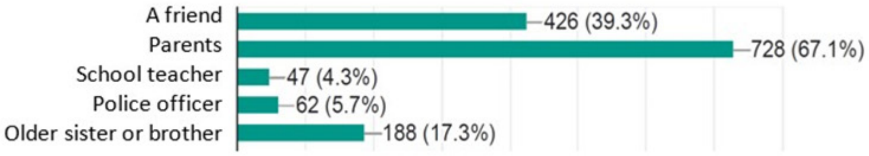
10. Do you know more about the internet then your parents?



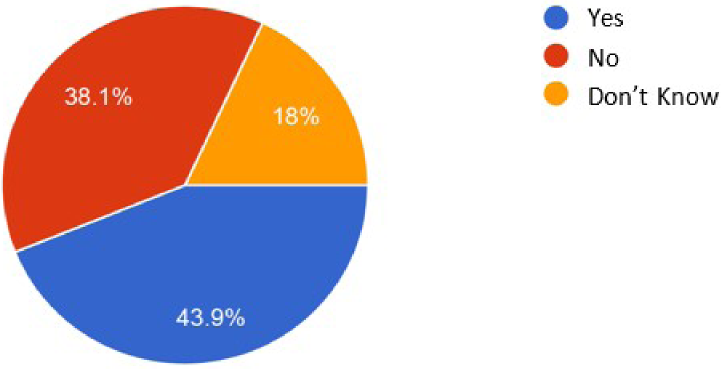
11. What worries you most about being online?



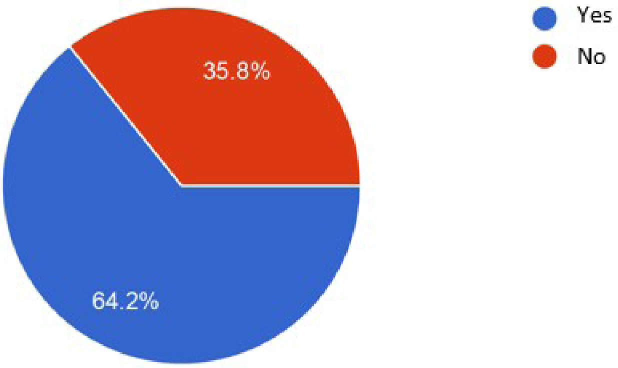
12. If you have a concern about anything online, who would you report it?



13. Have you had and awareness session about Online Safety?



14. If you answered Yes to the previous question who did the session?



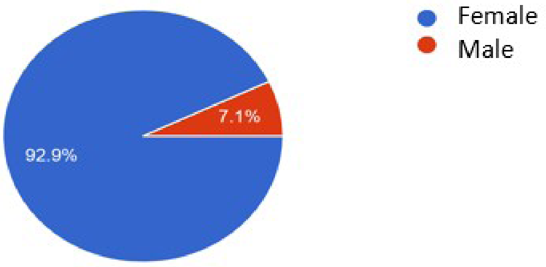
15. Have you ever seen anything on line that has made you feel upset?

Some of these questions have been taken from our long running online survey of children https://www.surveymonkey.com/r/ypinternet

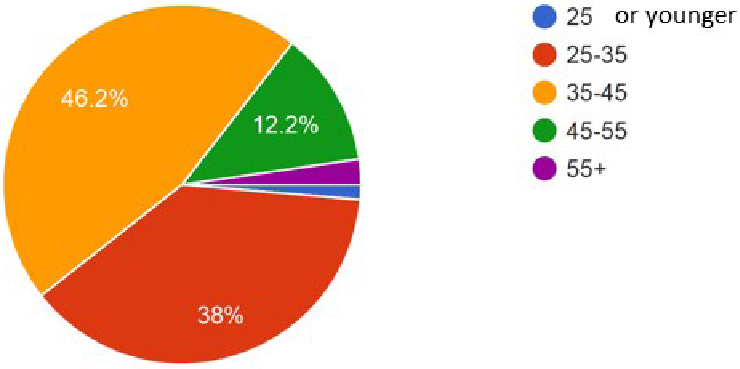
Appendix B: Parent online survey results

Questions for PARENTS

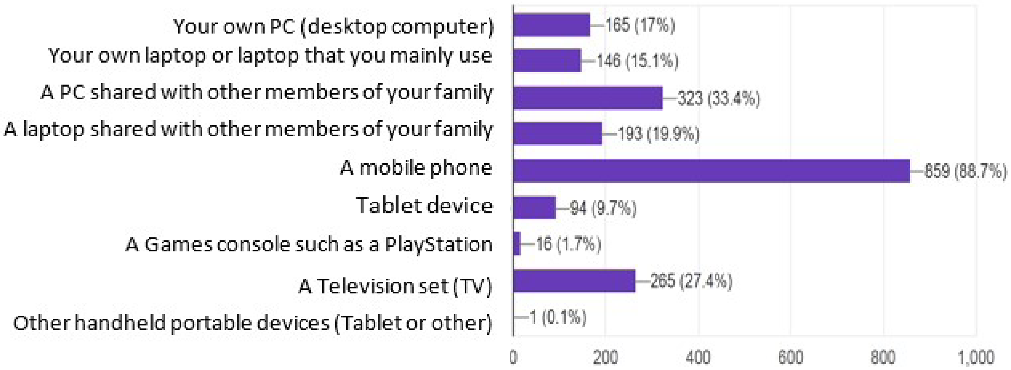
1. Are you



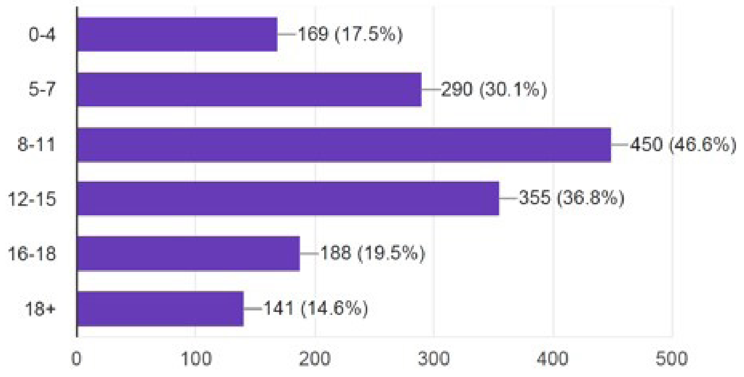
2. How old are you?



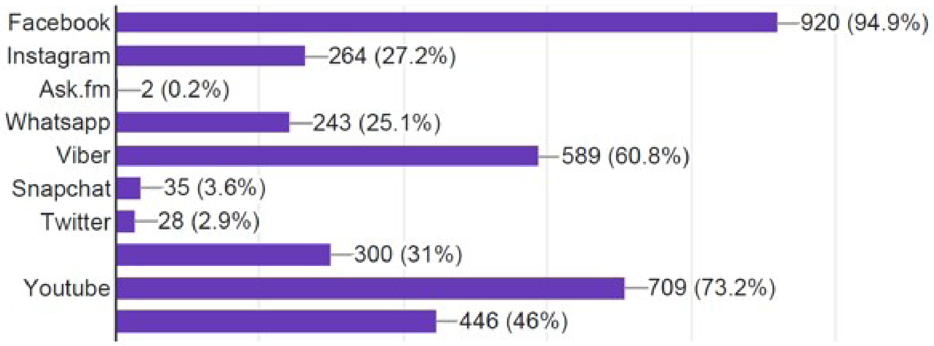
3. Which of these devices do you use for connecting to the internet? (tick all that apply)



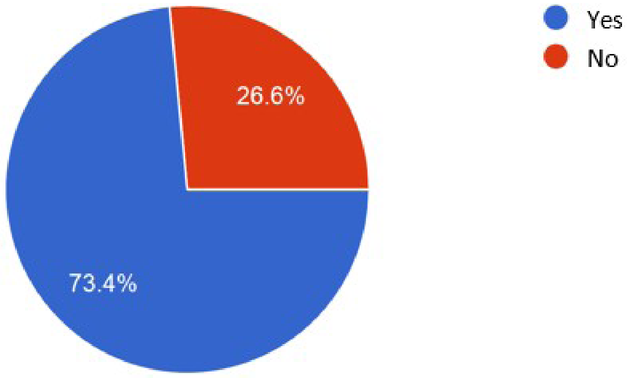
4. Age of your children



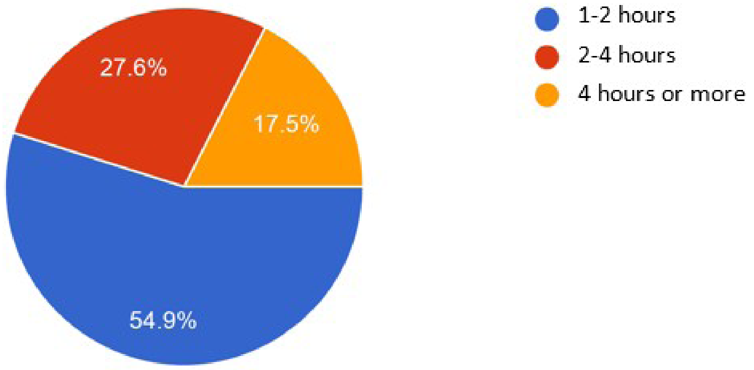
5. What of these online services/apps do you use? (tick all that apply)



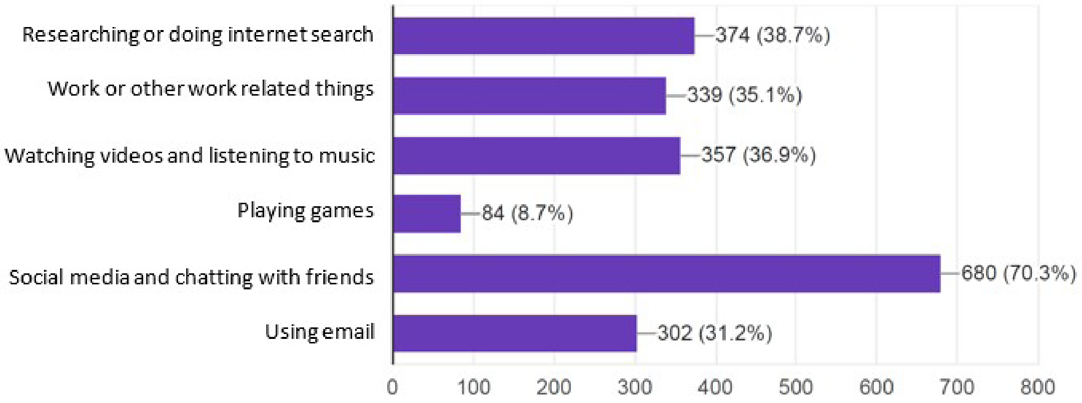
6. Do your children use social media?



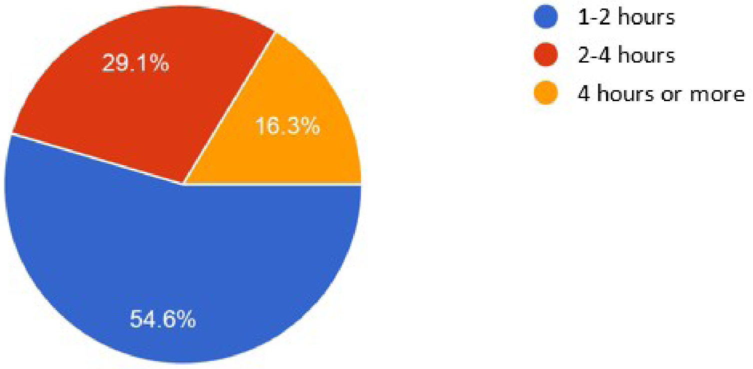
7. How many hours per day do you spend online?



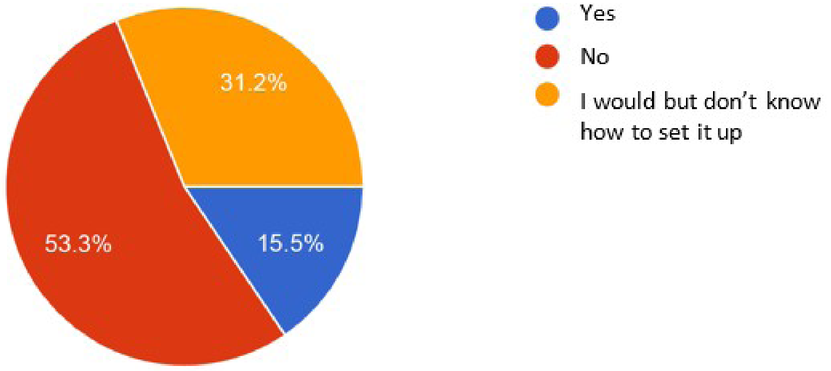
8. When you go online what do you most use internet for?



9. How many hours per day does your child spend online?



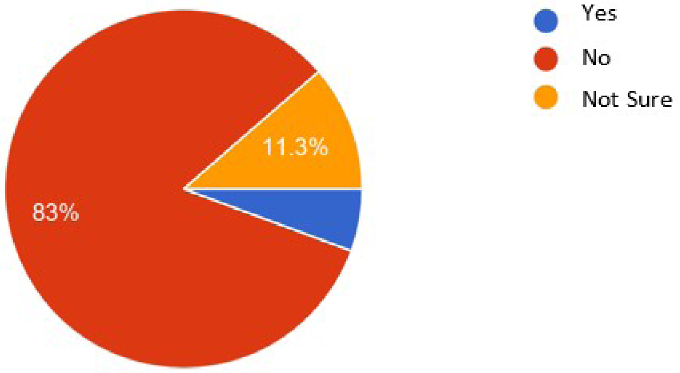
10. Do you use any filtering or monitoring software on any of your son/daughter's devices?



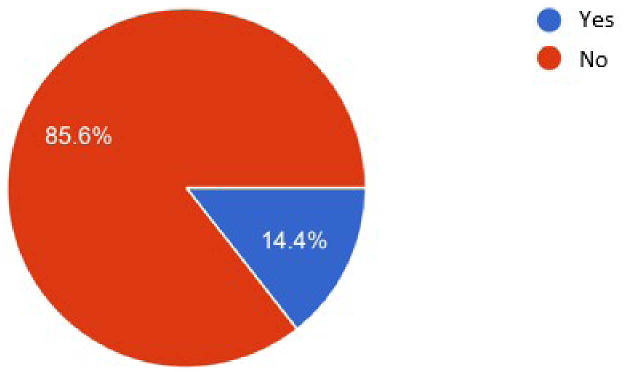
11. What concerns you most about your children being online?

- ○ Amount of time they spend online
- ○ Bullying
- ○ Commercialisation – ads, hidden cost etc
- ○ Exposure to inappropriate content
- ○ Fake news – accuracy of online information
- ○ Meeting strangers
- ○ Theft/loss of personal data
- ○ Other_______________

12. Have you or your child encountered an issue online?



13. If you have an issue online, do you know how and to who to report it?



Appendix C: Stakeholder online survey responses

Stakeholder online survey compiled responses

Stakeholders from across the country were invited to respond to a series of questions in preparation for the mission in October. The responses have been grouped and included within this document by agency type.

Georgia Innovation and Technology Agency

Question	Responses
1. To what extent is online safety and children's rights your responsibility?	GITA is not responsible for online safety and/or children's rights
2. How is online safety and children's rights integrated into your existing policies and processes?	
3. To what extent is online safety covered within existing legislation?	There is draft law "Online safety for children" (will be approved in 2018)
4. Which of the following areas do you focus? (Tick all that apply)	Public awareness of online safety, Education, Tools and Awareness, Information Security
5. What are your online safety priorities?	Cyber Hygiene, Awareness Raising Programs for Children, parents and educators; Trainings for school safety personal;
6. Please describe your activities to support online safety	Promotion of Startups in cybersecurity fields, awareness raising activities, lectures, Phishing-excercises etc.
7. Provide links to existing published work (eg policies, awareness, research, tools, legislation, programmes)	
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	GITA is preparing the awareness raising project which includes activities against the cyberbuliing in cooperation with the Ministry of Education and Ministry of Internal Affairs. Various activities (training, promotions, cyberweeks etc) will be implemented for students, teachers and school security personnel.
9. Can children/parents report online safety concerns or issues to you?	No
10. If yes – what sorts of reports do you accept and how can they do this?	
11. If no – how can children/ parents report concerns?	
12. Describe how you prevent and/or manage online child abuse content?	

Question	Responses
13. What initiatives or strategies would you like to see to improve online safety?	Awareness raising
14. What would you say are three key challenges in the online world?	Inappropriate conduct- Inappropriate contact-Inappropriate content.
15. What would you say are three key opportunities in the online world?	Connecting-broadcasting-posting
16. What other comments would you like to make?	

LEPL Data Exchange Agency Ministry of Justice of Georgia

Question	Responses
1. To what extent is online safety and children's rights your responsibility?	N/A
2. How is online safety and children's rights integrated into your existing policies and processes?	N/A
3. To what extent is online safety covered within existing legislation?	N/A
4. Which of the following areas do you focus? (Tick all that apply)	Public awareness of online safety, Education, Tools and Awareness, Data Protection, Information Security
5. What are your online safety priorities?	Our priority is to offer Cyber security services and activities to critical information system subjects, ministries, governmental organizations and private sector.
6. Please describe your activities to support online safety	We are organizing Cyber Olympiad for secondary school pupils and undergraduate students. Annually we are organizing trainings which includes 7 weeks of laboratory work in Cyber security. Our governmental computer emergency response team CERT-GOV-GE which is under LEPL Data Exchange Agency has a service- safe DNS Georgia. Every Georgian citizen can use this service with the use of which fishing websites, websites which contain malicious codes and websites which contain +18 content will be blocked.
7. Provide links to existing published work (eg policies, awareness, research, tools, legislation, programmes)	http://dea.gov.ge/?action=0&lang=eng On the link below you can find information about Cyber class and Cyber Olympiad which took start in 2014. It is an official Facebook web-page of CERT-GOV-GE you can find information, photos and media content: https://www.facebook.com/certgovge/?ref=bookmarks

Question	Responses
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	We implemented Cyber incident management system and during the cyberattack they can report cyber incident 24/7 to us. In case of public and private partnership we have created Georgian cyber security forum which is conducted annually. The representatives of cyber security specialists, information security managers from public and private sector attend the annual cyber security forum. The main goal of this forum is to secure Georgian cyber space and identify problems and risks of Georgian cyber space.
9. Can children/parents report online safety concerns or issues to you?	No
10. If yes – what sorts of reports do you accept and how can they do this?	N/A
11. If no – how can children/ parents report concerns?	No
12. Describe how you prevent and/or manage online child abuse content?	We are working on Cyber security incidents of organizations not specifically for child abuse issues.
13. What initiatives or strategies would you like to see to improve online safety?	It will be beneficial to introduce Cyber hygiene and Cyber bulling educational programs in secondary schools. It will also be helpful if government will support Internet service providers in Georgia to implement parental control service.
14. What would you say are three key challenges in the online world?	Cyber bulling, cyber-attack, awareness.
15. What would you say are three key opportunities in the online world?	Increase awareness, cyber education, cyber protection strategy.
16. What other comments would you like to make?	Nowadays it is extremely important to have online safety strategies.

Ministry of Internal Affairs of Georgia

Question	Responses
1. To what extent is online safety and children's rights your responsibility?	"112 Georgia, an Emergency and Operative Response Center under Ministry of Internal Affairs of Georgia is the key agency dealing with the emergency service management with two call centers, which receive emergency calls from all over Georgia 24/7. 112 Georgia was founded in 2012 with the aim of unifying the emergency number for Police, Fire/Rescue and Ambulance services. Before 2012, the respective services were available through dialing three different emergency numbers, which would usually cause confusion among the citizens, thus increasing the time of emergency response. The fundamental purpose of LEPL 112 is to protect Human Rights, as well as children's Rights."

Question	Responses
2. How is online safety and children’s rights integrated into your existing policies and processes?	LEPL 112 has the special policies and standards when kids are the call initiators. We conduct special training for new recruited call-takers about above mentioned standards. These components are integrated into the investigation process.
3. To what extent is online safety covered within existing legislation?	N/A Basically, online security issues are envisaged by the legislation, but there are some flaws.
4. Which of the following areas do you focus? (Tick all that apply)	Tools and Awareness, Data Protection Law enforcement
5. What are your online safety priorities?	We collect and protect all the information of cases and call initiators data among them children call initiators which are in emergency situation. To fight against chuld abuse and protect personal data.
6. Please describe your activities to support online safety	N/A My duty is to investigate and prevent cybercrime, which is somewhat connected to online safety.
7. Provide links to existing published work (eg policies, awareness, research, tools, legislation, programmes)	N/A For us it is important awareness, programs and tools.
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	"MoU was signed between the Emergency Response Center of Ministry of Internal Affairs of Georgia – 112 and Education Management Information System (EMIS) of Ministry of Education and Science of Georgia. According to the MoU, through EMIS database – eSchool, call takers of 112 will have an opportunity to instantly determine the residential address of the school children and the contact information of their parents by inputting their name or school information into the database. This novelty is especially important in cases, when school child is unaware of his/her address, but knows the name and number of the school he/she goes to. The information is transmitted through closed network, which implies that the transferred data will be fully protected from the outside access. Only the call takers of 112 will have access to the database and only in cases, when school child is unable to name the exact address. MoU between the two entities will reduce the operative response time during the emergencies, when the school child is in need and every second counts." We cooperate with media to give the citizens information about cybercrime and iinformation how to protect them from the hackers.
9. Can children/parents report online safety concerns or issues to you?	Yes Don’t know
10. If yes – what sorts of reports do you accept and how can they do this?	There are some notifications from parents and neighborhoods about the children in non-secure situation, which are collecting and transferring to relevant agencies (Police, Ambulance, Fire).
11. If no – how can children/parents report concerns?	Children or parents may contact us if they think that the crime was committed against them.

Question	Responses
12. Describe how you prevent and/or manage online child abuse content?	We are investigating child abuse cases.
13. What initiatives or strategies would you like to see to improve online safety?	Media and Awareness raising campaigns, Internet users Standards, Develop the relevant strategy documents and policies, Improve the knowledge and skills of parents, teachers, educators.
14. What would you say are three key challenges in the online world?	Lack of information and awareness of society, easy access to Internet (social media) and lack of regulations. 1. Child abuse; 2. Illegal extraction of personal data; 3. business email compromise.
15. What would you say are three key opportunities in the online world?	Assessment of the existing situation, develop the relevant regulations and monitoring the process of implementation 1. International cooperation; 2. Cooperation with the private sector; 3. Cooperation with media.
16. What other comments would you like to make?	LEPL 112 express the interest to involve safety Internet strategy project, upgrade the existed standards, building capacity for call-takers and deliver media campaign in regions.

Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia

Question	Responses
1. To what extent is online safety and children's rights your responsibility?	Our department works in social affairs field, children rights, determines state policies on childcare system, develops social security state programs and etc. Our role in online safety is to give information about online safety children, who is in childcare services or with whom the social service agency works.
2. How is online safety and children's rights integrated into your existing policies and processes?	Procedures of child protection referrals includes online child safety issues (Order N437 by Government of Georgia on the Approval of the Child Protection Referral Procedures 12 September 2016, Tbilisi).
3. To what extent is online safety covered within existing legislation?	There is a law about information security which sets general standards for information security for public and private sectors. The goal of the child protection referral procedures is to protect the child from all forms of violence in family and outside of family settings through establishing an efficient and well-coordinated referral procedures system.
4. Which of the following areas do you focus? (Tick all that apply)	Child protection.
5. What are your online safety priorities?	Information security, law enforcement, legislation.
6. Please describe your activities to support online safety	To teach children about different techniques and ways how to follow online privacy.
7. Provide links to existing published work (e.g. policies, awareness, research, tools, legislation, programmes)	Booklet

Question	Responses
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	We conduct trainings on this issue and collaborate with NGO and International Organizations in Georgia. When there is a case where child is abused, bullied or etc. LEPL Social Service Agency begins working with child and family and child receives psychological service.
9. Can children/parents report online safety concerns or issues to you?	Yes
10. If yes – what sorts of reports do you accept and how can they do this?	With Referral from school/police and National hot line
11. If no – how can children/parents report concerns?	
12. Describe how you prevent and/or manage online child abuse content?	We give children information about online abuse and print educational brochures about prevention and how to protect themselves from this.
13. What initiatives or strategies would you like to see to improve online safety?	There could be national strategy about distributing and uploading child Pornography online and online web sites would protected from unusable/abusive information.
14. What would you say are three key challenges in the online world?	Social media, children pornography and dangerous Internet
15. What would you say are three key opportunities in the online world?	Legislation, Policy and information
16. What other comments would you like to make?	

Non-governmental organization (NGO)

Question	Responses
1. To what extent is online safety and children's rights your responsibility?	• It is not my direct responsibility but I think it is very important • Green Internet is a non-governmental organization with the aims to control and regulate Georgian Internet space and to prevent the unlawful and fake information from spreading out through social networks and media. Our team is working actively to protect our Internet users from threats and dangers which may be caused by using the Internet.
2. How is online safety and children's rights integrated into your existing policies and processes?	• Not really • We are carrying out training and presentations in different places. For instance, we have held meetings for teachers, children and their parents in several schools in order to supply information about Internet security. Soon, we are going to hold more and more meetings not only in the schools of capital city of Georgia but in the regions of the country.
3. To what extent is online safety covered within existing legislation?	• It definitely needs improvement • Internet space is too unregulated in Georgia, especially, there is no special law for Internet-security.

Question	Responses
4. Which of the following areas do you focus? (Tick all that apply)	• Public awareness of online safety, Education • Public awareness of online safety, Education, Regulation, Legislation/ Policy, Producing positive online content, Child protection, Research, Information Security
5. What are your online safety priorities?	• Information Security • Our priorities is to protect society, especially children and their parents from illegal contents, such as "deadly" online games, pornography, cyber bullying, etc.
6. Please describe your activities to support online safety	• Awareness rising, development of online tool for student that will support students and interested persons to improve their skills in cyber-security • As it was mentioned above, we are carrying out training and presentations in several schools and universities. we also want to deliver filter in order to protect children. Moreover, we are working to establish hot line which will help people who are harmed by illegal contents.
7. Provide links to existing published work (eg policies, awareness, research, tools, legislation, programmes)	• https://www.cyber-lab.tech/
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	• GRENA is technically support universities in case of cyber incidents and sending information about vulnerabilities. • We have collaboration with Ministry of Internal Affairs, Georgian National Communications Commission, Parliament of Georgia, Ministry of Education and Science, etc.
9. Can children/parents report online safety concerns or issues to you?	• No • Yes
10. If yes – what sorts of reports do you accept and how can they do this?	• Children and their parents can contact us on our organisation's face book page.
11. If no – how can children/ parents report concerns?	

Question	Responses
12. Describe how you prevent and/or manage online child abuse content?	• As it was mentioned, we have held presentations to different schools in order to raise children's awareness. Also, we have meetings with representatives of Parliament of Georgia and Georgian National Communications Commission. We discussing Internet-security legislation issues. • I have the appropriate conversations with children and parents to be able to control their children so that no one can abuse the child in online relationships.
13. What initiatives or strategies would you like to see to improve online safety?	• Our wish is to establish hot line, create effective and proper legislation for Internet-security and introduce filter to the country. • "Access to database access is required. Organize access control of fossil data."
14. What would you say are three key challenges in the online world?	• Fake news 2) Cyber bullying and cybercrime (including Cyber terrorism) 3) "Deadly" online games • "Child Rights Protection, Online security enhancement E-mail and web-page information protection"
15. What would you say are three key opportunities in the online world?	• To raise awareness of Society 2) To adopt effective legislation and ensure law enforcement 3) To control and detect illegal contents • "Communication, • Reliable information space, • Freedom of Information."
16. What other comments would you like to make?	• No

Schools

Question	Responses
1. To what extent is online safety and children’s rights your responsibility?	• I believe that my responsibilities are really high on online security because the students have access to the Internet, so I often have conversations with them about online security. • On high level • ONLINE SAFETY AND CHILDREN'S RIGHTS ARE PROTECTED BY OUR RESPONSIBILITY • Significantly • To get more information and recommendations in the field of children's online security in order to more efficiently manage and prevent the processes • I am librarian at the IB school. Our students do a lot of research and it is my responsibility that they are safe during the research. • Control the work of the pupils in the Internet • As a parent online safety and children's rights are the most important thing that will be always parent responsibility. • I always control online safety when I use the Internet during classes • Creating a safe learning environment • School takes responsibility for the matter. • At school Internet sites are limited, so that children cannot visit every sites • We control the school more or less • Online safety of children is protected at school • Our school staff has great responsibility for online safety and children's rights at school. • As I am a school programme coordinator I am in charge of creating policies along with my colleagues. • High responsibility • School stuff takes care that the children can`t use the mobiles during teaching process. In computer labs students know that they only **h**ave access to relevant sites. • Less protected • It is totally our responsibility. • The child's rights are protected in our school. • We are responsible for online safety and children's rights. The ability for young students to use online tools effectively and safely provides both a skill for life and the means to acquire new skills. • As a school director I am responsible for the students' rights and safety in school area. • Children should understand. • Always. • "The pupil should never give personal information on different web sites, including telephone numbers, school and home addresses, parents' jobs, email addresses. • Everything is my responsibility to protect children" rights. • Online safety and children’s is all our responsibility • I try to do best for my students to have safety online.

Question	Responses
2. How is online safety and children’s rights integrated into your existing policies and processes?	• I often speak to students about their access to certain sites, they know their rights as well as in the school and outside the Internet. As well as the threats that are somewhat connected to the use of the Internet. • In our school labs we have limited rights in the name of safety and so is the information given to the children about this • The Ministry of Education provides online safety and children’s rights and they are integrated into existing policies. • Integrated into the teaching process. • Pupils are provided with periodic meetings and conversations about their rights and risks that may harm their security • I test the history of the sites used by the students and keep track of the rights of the students • These are the parts of politics and processes and I cannot see existing politics without children's care and online safety. • In order to keep children's safety all social networking sites are unavailable • In the course of study we create a safe and free learning environment for pupils with the encouragement of school administration teachers and class leaders • The pupils are restricted in the course of the lesson if they do not consider the need for educational process. The school WiFi is restricted to students and blocked by web pages that are not used in the learning process and are in danger for juveniles • Children can use only educational sites • Online-safety in the school is mainly protected by the teacher's monitoring, students learn safety policies. • Online safety and children's rights are quite integrated into our existence policies and processes. • It is part of it. And we are in charge of monitoring it. • To make locked unuseful websites. • Children can`t open all the sites that may contain danger for them. The sites are blocked from the Ministry of Education. • Not enough. • It is integrated and stated in our mission of the school. • The child's right is compatible with the school's legal basis and relationships. • We provide children with means through which they can exchange information, be entertained, socialize, do their homework and classwork and do research. • "It is integrated in both, as online networks (Facebook, twitter, etc.) not connected to school process is not available for students at school. The school policy also based on specific regulations." • Currently do not have. • Regularly provide student's the rights and online safety rules. • Online safety and children’s rights is integrated and controlled by us. • Online safety is not protected. • It is safe for children at school.

Question	Responses
3. To what extent is online safety covered within existing legislation?	• As is known, the most common types of cybercrime are: Internet fraud, theft, unauthorized access to the computer system, unauthorized use of computer systems and data. The law, of course, prohibits. The Criminal Code of Georgia is regarded as a cybercrime by an unlawful act involving at least one component of the 284th and 286th Articles of the same Code. • On high level • ONLINE safety is covered in high level but it depends how the organization fulfils it • Partly • The legislation is less focused on online security issues • The current legislation provides for the protection of the Internet use, but I think it should be more flexible and focused on the student. • All suspicious sites are blocked • The pupils are restricted in the course of the lesson if they do not consider the need for educational process. The school WiFi is restricted to students and blocked by web pages that are not used in the learning process and are in danger for juveniles • Online safety-security perimeters require strengthening. • Online safety is covered with existing legislation. for example children have access only educational programmes at school computer labs. • Installing filters and anti-virus • The ministry of education takes responsibility for this • Password protected • It is in accordance with the existing legislation. In addition, we have banned access to some social sites. • Safety is maximally customized for the needs of the pupils, works with the resource officers, the school regulations are enacted, the classmates have a constant communication with their parents. • Our existing legislation includes some points concerning online safety and children's rights. • At school students are not allowed to use online network, except study purposes. School policy regulates it. • N/A • In order to avoid unauthorized access to the system, maintain the accuracy of data, ensure proper use of data. • I think the whole school area is covered. • There are many cases of teenagers when it comes to online security vulnerability.

Question	Responses
4. Which of the following areas do you focus? (Tick all that apply)	• Public awareness of online safety, Media Literacy, Law enforcement, Tools and Awareness, Legislation/Policy, Producing positive online content, Child protection, Data Protection. • Public awareness of online safety, Education • Public awareness of online safety, Education • Public awareness of online safety, Education, Media Literacy. • Public awareness of online safety, Education, Law enforcement, Legislation/Policy, Child protection, Information Security. • Public awareness of online safety, Education, Regulation, Producing positive online content, Research. • Public awareness of online safety, Education, Media Literacy, Law enforcement, Tools and Awareness, Regulation, Legislation/Policy, Producing positive online content, Child protection, Research, Data Protection, Information Security. • Education • Public awareness of online safety, Education, Tools and Awareness, Producing positive online content, Child protection, Research. • Public awareness of online safety, Education, Child protection, Data Protection, Information Security. • Public awareness of online safety, Tools and Awareness, Child protection, Information Security. • Education, Media Literacy, Tools and Awareness, Regulation, Child protection, Information Security. • Education • Public awareness of online safety, Education, Media Literacy, Law enforcement, Legislation/Policy, Producing positive online content, Child protection, Data Protection, Information Security. • Education, Media Literacy, Tools and Awareness, Child protection, Information Security. • Education • Public awareness of online safety, Education, Tools and Awareness, Child protection, Research, Data Protection, Information Security. • Education, Media Literacy, Producing positive online content, Child protection, Research, Information Security. • Education, Media Literacy, Regulation, Legislation/Policy, Child protection, Research, Information Security. • Public awareness of online safety, Education, Media Literacy, Law enforcement, Producing positive online content, Child protection, Data Protection, Information Security • Education, Media Literacy, Regulation, Producing positive online content, Child protection, Information Security. • Public awareness of online safety, Education, Tools and Awareness, Regulation, Producing positive online content, Child protection, Research, Data Protection, Information Security. • Education • Education, Producing positive online content • Education

Question	Responses
	• Public awareness of online safety, Education, Media Literacy, Law enforcement, Tools and Awareness, Regulation, Legislation/Policy, Producing positive online content, Child protection, Research, Data Protection, Information Security. • Education, Media Literacy, Child protection, Information Security • Public awareness of online safety, Tools and Awareness, Child protection • Public awareness of online safety, Education, Media Literacy, Law enforcement, Tools and Awareness, Producing positive online content, Child protection, Information Security.
5. What are your online safety priorities?	• "Protection of confidential information, • Personal data protection, • Creating Safe Functional Systems." • To defend children from undesirable information • To protect children from undesirable information • Children's physical security • Protect students from harmful effects of cybercrime and undesirable information. • Personal Data Protection • Care • Provide awareness of online safety • Creating a safe and free learning environment for children • We have years of experience in developing online security technology, we consider Safe Browsing technology as a priority. • Cyber-bullying prevention in pupils • Security policy tightening and more monitoring • We provide useful overviews on a range of online safety issues – such as cyberbullying, sexting and self-harm. • To make firewall • The students must be in safe environment • Protecting pupils from harmful influences • To ensure the safety of children's personal data. • Our online security priorities are to protect the personal safety of any person in this area. • Our online safety priority is to implement the scheme for the rapid removal of material that is harmful to a child. • Not to make students use Internet for abuse. • Personal accounts are protected • Yes • Be a good citizen of online space Never do the things that will harm or offend another person. • Our online safety priorities are that we can control our children well. • Law enforcement • To be children protected from bulling.

Question	Responses
6. Please describe your activities to support online safety	• My activities are limited to providing online safety in the field of work with students. • We do presentations, watch them films about safety and we talk about danger of this problem. • Make presentations, show films about dangers of cyber safety. • Providing information • Regular meetings with parents are associated with free online space threats. We give advice and recommendations about the students' online space and the proper use of the Internet. • Control the work of the pupils with their age and interests related websites. • I always follow new coming programmes and use them to support online safety. • I check all sites before introducing • We are conducting monitoring to eliminate the facts of violence against children. We are working on the prevention of bullying. • "1. The simplest and most effective method of securing non-public information and information on the system (which cannot solve all problems, even because there are many different web technology / platforms and one is not enough) is a prohibition of executing scripts (JavaScript). • 2. java and other platforms (Adobe Flash). • 3. It is possible to get another size. HTTP protocol, which is the basis of data exchange and communications on the Internet, has a function called do-not-track (DNT). This feature should be turned on from your browser, after which your browser will tell you the web site that you do not want to give it (the website) information on how you get it. Keep in mind that part of the websites (server) can ignore your desire and still be aware of how you come with it." • Conversations with pupils, meetings with parents, polls, providing information. • Conduct lessons, show movies on bulling, hold discussions, implement projects, trainings. • We get to know the websites which provide excellent information for children, parents and teachers. • Doing servers and filters of the web • We observe the usage of technologies that have access to the Internet • Password, code enclosure, dissemination of information on threats. • We have a password. • Our support is expressed through the password system and the policy of non-intervention in the student's private space. • A prevention group exists to consider the effects of Internet use on children as well as to deliver online safety education. • Organizing meetings with parents and children, giving them important information on the problem. • Systematically we inform students • Should be safe for children

Question	Responses
	• Be cautious and think about who you send a photograph. Anyone may have your photo for wrong purposes or abuse • Use it. • Say to your parent or trusted older man if you find information that makes you feel uncomfortable. • Ask your teacher or parent before downloading any programme, install or do something. • Which can damage your computer and threaten your family's personal information. • When registering in the Quick Messenger (IM) on the social network, set the options that make your page "private". • I have never say our password to anybody. • Public awareness of online safety • I can only have monitoring at my lesson.
7. Provide links to existing published work (eg policies, awareness, research, tools, legislation, programmes)	• I provide the acquisition of published materials for pupils and parents. • We have no published works on this level • Nowadays we have no links • https://www.facebook.com/%E1%83%93%E1%83%90%E1%83%91%E1%83%90-%E1%83%90%E1%83%93%E1%83%98%E1%83%92%E1%83%94%E1%83%9C%E1%83%98%E1%83%A1-%E1%83%A1%E1%83%90%E1%83%AF%E1%83%90%E1%83%A0%E1%83%9D-%E1%83%A1%E1%83%99%E1%83%9D%E1%83%9A%E1%83%90-1065647550118700/ • https://privacy.google.com/intl/ka/safer-internet.html • Google, Wikipedia, YouTube. These are the links I use them every day. • https://softlinegeorgia.ge/ • Ensure more privacy and privacy of existing published links, strengthening confidentiality (for example, politics, informing, research, tools, legislation, programs). • Kaspersky. dr web... • Access to educational programs in school space, blocking the rest; • tbilisiskola108.blogspot.com • Find the info on the webpage: http://gtstudioorg1.ipage.com/sites/school3/ • We have never recorded this kind of work. • N/A • Policies, programmes • Yes • None of them.

Question	Responses
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	- We make our pupils watch films about this problem - We are provided by links to improve online safety - The school actively cooperates with the police, the Prosecutor's Office of Georgia, the Social Service Agency. Their representatives, children's inspector, social worker, inspector investigators systematically meet pupils and arrange lecture with them - I mostly cooperate with the websites of the Ministry of Education - I do not work with other agencies and organisations. - In case of problem I contact them - Meeting and trainings can be planned remotely. - We are trained how we get rid of cyber bullying, copyright and plagiarism, protecting personal information, information literacy, online security. - Making firewalls and lock by mikrotik router - They block the sites may be unsafe for the children. - The school serves an LEPL Educational Management Information System, which works quite efficiently - We have constant contacts with those organizations and institutions who are interested in our school life. And this relationship is mainly done through online platforms - We cooperate with university personnel (psychologists) and they deliver different seminars and workshops for students. Also, mandatory service helps us greatly to manage with it. - We cooperate with the Ministry of Education - Do not work - We have - I am just a teacher, I give the students the information, But I think the policy should take care of the safety of the students - I don't work with other agencies.
Question	**Responses**
9. Can children/parents report online safety concerns or issues to you?	- Yes from 20 respondents - Don’t know from four respondents - No from four respondents

Question	Responses
10. If yes – what sorts of reports do you accept and how can they do this?	• By summing up our discussion and by filling questionnaires • By filling questionnaires • Verbal talks • Parents say that they do not know what kind of information they receive, and it is difficult to control the time spent in the online space, as well as online games where actively involved in the relevant bodies of the Ministry of Interior • In this case, I know the problem and I try to help him • Individual meetings and conversations • We start the investigation and if the problem is beyond the school, then we will put the police in the course of the case. • The head of the sixth class was informed by her students/boys and one of their parents that they are threatened online by the boy from the other school. • Any sort of • They can do it personally. • Orally, via email, meetings; • Basically, information is made through the classroom created by Facebook • We cooperate with the parents and their children and accept all sorts of reports by our Facebook page. • Any kind of reporting for is acceptable for us, but we have had no reports yet. • Professionals should talk to children about the harmful effects of the Internet • Don't have an answer • Be careful when using photos of other (especially unknown) people • You agree to appear on the photo. • Send only messages that you would like to receive.
11. If no – how can children/ parents report concerns?	• Do they independently or ask others • They should have a programme and then they can do a good and right report. • We can contact a responsible person, such as a parent, caregiver. Many websites, including Windows Live Messenger and Facebook, include the button CEOP button that directly connects children's exploitation and Internet Security Centre. • Personally, at meetings; • Orally or written forms is acceptable. • Don't have an answer • Parents and children should be informed They should be able to declare a possible danger • I have no information about it.

Question	Responses
12. Describe how you prevent and/or manage online child abuse content?	• I have the appropriate conversations with children and parents to be able to control their children so that no one can abuse the child in online relationships. • We limit our children's accessibilities • We limit children's access to Internet • Blocking certain sites • Give children a definite time for online space, and set limitations on full access to the online space (for example, a parent has a code or a password that will allow a child to unblock or unleash a certain online space) • I did not have a similar case • First of all every child should have a good education and he/she should understand what programme to use. • Providing information • Preventive measures • Students at school have access to educational Internet resources and more or less we control the situation • We recommend children do not respond, and inform parents and schools. • The head of the class informed about it the head of the school where the boy studied, she also asked her students/boys to cancel and not to be the member of the group where the boy of the other school can abuse them. So, in this way we managed getting rid of future online children abuse. • By Kaspersky anti-virus • Class mentors take care / supervise their classes. • I did not have such a case; • Send a massage to parents • We did not have such a case • An advice platform exists with guidelines for parents about the appropriateness of online content. • We have had no real experience yet, only school policy exists. actually, it is a great problem to cope with it. • Show a case of real situation or interact with non-extracurricular activity. • Tracking • Block any person with whom you do not want to speak. If you do not know how to do it, ask a teacher, parent or trusted friend. • I have many reasons to prevent online child abuse content, to avoid everything bad. • All of these sites should be blocked, Parents should be careful, The government should be cared for and checked, The law should act against criminals • I had not have this problem.

Question	Responses
13. What initiatives or strategies would you like to see to improve online safety?	• "Access to database access is required. • Organize access control of fossil data." • We need information about this from other countries and meetings with them to share information • We need information and meetings with different organisations • Online spaces are strictly controlled and are limited in practice • I would enhance the control over the pupils' work in the Internet • Programmes which are effective and educative. • To get more information about online safety and share it with school community • Conversation with pupils and their parents and joint activities with pupils' participation of different ages • "1. The classroom Internet Security Agreement; 2. Security strategy; 3. Use SchoolTube, Video Site. 4. It is the door policy- Cyberbullying; " • Confidentiality, Access to Information, Introduction to Internet Label for Students and Parents • There is a need of strengthening confidentiality protection policy • 1.Create Complex Passwords. 2.Keep all our software updated in order to have the latest security patches. • To make server room and all the firewalls • It would be desirable to prepare video trainings and information managers • To have the possibility to block the specific pages that may be dangerous for pupils • Online security strategies should be developed, but it is probably competence of prerogative bodies. • A specific scheme should exist to regulate illegal and offensive online content. • To organize different informative events that will really help the school staff as well as the students and parents to raise awareness in the field. • Students should receive information from both professionals and peers • To improve online quality. • Develop any law for online offenders • I have no information about this.

Question	Responses
14. What would you say are three key challenges in the online world?	• "Child Rights Protection, • Online security enhancement • E-mail and web-page information protection" • Danger of bulling and breaking our accounts • Danger of bulling and breaking our accounts • Cybercrime, 2. Free space 3. The correctness of the information • Safety, bullying, false information • Games, chats, meetings. • Yes, there are. Social networking sites • Security, personal data inviolability, cyberbullying • Cooperation, communication and monitoring • 1.Online learning has become very widespread, it has many disadvantages such as, students feel isolated from the instructor and there is no interaction between them. 2.Slow Internet connections or older computers may make accessing course materials frustrating. 3. Managing computer files and online learning software can sometimes seem complex for students with beginner-level computer skills. • To find programmes that blocks bad websites • The videos that contain the information that must not be available for the students for all age, online games that contain the violence. • Blocking unethical, threatened websites disappear from Internet space • Cyber bullying, media bullying, lack of protection. • Online security challenge can be fake news, hacker attacks and human indifference • Three key challenges in the online world are development, regulation and success. • No information, no regulation and no awareness. • Information exchange and reception are conducted quickly, easily and efficiently. • No one can write or post anything that is not desirable to see children • I think online net must not be very loaded. • Correct and timely informing, Protection programs, Security Policy • I have not information.

Question	Responses
15. What would you say are three key opportunities in the online world?	• "Communication, • Reliable information space, • Freedom of Information." • We can do everything by using Internet with no language barrier • We can do everything by Internet with no language barrier • Quickly Find Information 2. Effective Communication 2. Publicity • Fast Internet service, availability of information, diversity • Self-education, distant study, making new friends • Awareness, effective communication, saving time • 1.Students can study anywhere they have access to a computer and Internet connection. 2. Develops knowledge of the Internet and computers skills that will help learners throughout their lives and careers. 3. Successfully completing online or computer-based courses builds self-knowledge and self-confidence and encourages students to take responsibility for their learning. • To make programs for making safe web and pc's • It's the source of information in any educational field that saves our time and energy and money. / Internet is the way to contact close people. • Internet space should serve the needs of the population, adolescents to healthy lifestyles, health care and educational directions • Fast rate communication, effectiveness and quality performance • Quick quality access to information, access to news, human contacts • Three key opportunities in the online world are borderless information, a large amount of opportunities and unlimited possibilities. • Information, learning things and socializing. • Getting large volume information in a short period of time. • We can use the Internet to talk with each other and find relevant information • You can contact to anybody very fast, to reach all kinds of materials, maps, books. • Correct and timely informing, Protection programs, Security Policy • I have not information.

Question	Responses
16. What other comments would you like to make?	• No • No comments • No comments • Thank you for cooperation • Providing more information about schools online safety issues • I can share my experience and others to share with me • Healthy living, nutrition shall be promoted, scientific- popular news propaganda; • We do not have recommendation at this stage • The problem is really controversial, vitally important to avoid some life problems and difficulties that are sometimes bring fatal results. • It would be good if safety rules are developed • I would say to be very protected from everybody and everything. • The correct security policy is needed • I want to have more information how I can have safe online for my students.

Social services agency

Question	Responses
1. To what extent is online safety and children's rights your responsibility?	The SSA is central body of guardianship and care in Georgia, therefore it is responsible for taking actions on the cases of the violence of the rights of children or abuse. The agency is also one of the main bodies in the referral system of children violence.
2. How is online safety and children's rights integrated into your existing policies and processes?	The Agency is responding to respond to all types of messages about the cases of children abuse and it is correspondingly reflected in all policy and procedural documents
3. To what extent is online safety covered within existing legislation?	N/A
4. Which of the following areas do you focus? (Tick all that apply)	Child protection
5. What are your online safety priorities?	N/A
6. Please describe your activities to support online safety	We are acting according to the case requirements
7. Provide links to existing published work (e.g. policies, awareness, research, tools, legislation, programmes)	
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	The procedures of cooperation among the agencies and organizations in the sphere of childcare are described in the Decree of the Georgian Government 437 (2016).

Question	Responses
9. Can children/parents report online safety concerns or issues to you?	Yes
10. If yes – what sorts of reports do you accept and how can they do this?	Any type of reports are accepted
11. If no – how can children/ parents report concerns?	N/A
12. Describe how you prevent and/or manage online child abuse content?	According to the existing legislation
13. What initiatives or strategies would you like to see to improve online safety?	First of all international learning of experience would be needed
14. What would you say are three key challenges in the online world?	1. The area is very broad, 2. Mechanisms of control of the Internet, 3. Low level of information of guardianship and care givers
15. What would you say are three key opportunities in the online world?	Timely provision of information to children on understandable language, establishment of unified mechanisms for the protection of children in online
16. What other comments would you like to make?	

Telecom

Question	Responses
1. To what extent is online safety and children's rights your responsibility?	• Part of Online safety is in my responsibility, children's rights is not in my job description list. • There is no designated person or specific organizational unit within our organization dedicated to the children's safety issues. • I am the Head of the Information Security Department of Silknet and my responsibility is to coordinate efforts in protecting company from Information security threats. Online safety is the considerable part of this work. • As an SME association and ISPs business organization it is directly related with my members interests and responsibilities.

Question	Responses
2. How is online safety and children's rights integrated into your existing policies and processes?	• We have strong online safety policies implemented and we are continuously working on improvement of that policies. Currently, our company does not offers child's protection to customers, but there is ongoing project, to implement parental control system, which will help our customers to secure children from online threats. • Our organization is in compliance with all rules and regulations required by the relevant authorities including policies related to the online safety in general. • We implemented different types of security polices and corresponding instructions. • We did service contract for my members and also adopts Code of Conduct for non-regulated areas with support of CoE. We also launched project and you can find more info there www.stopline.ge.
3. To what extent is online safety covered within existing legislation?	• From my point of view, current legislation in Georgia is not covering enough online safety. • Telecommunication service providers are required to adhere to the rules and instructions set and issued by Georgian National Communication Commission regarding the admissibility of the content hosted on various websites and/or online resources, including those related to the online safety and children's rights. • Partially. • It is very general but we have good case law.
4. Which of the following areas do you focus? (Tick all that apply)	• Education, Child protection, Research, Data Protection, Information Security. • Public awareness of online safety, Tools and Awareness, Regulation, Legislation/Policy, Research, Data Protection, Information Security. • Public awareness of online safety, Education, Media Literacy, Regulation, Data Protection, Information Security. • Public awareness of online safety, Education, Media Literacy, Tools and Awareness, Regulation, Legislation/Policy, Producing positive online content, Child protection, Data Protection, Information Security.
5. What are your online safety priorities?	• Protect children from inappropriate content, Protect personal privacy. • Making Internet safer for our fixed and mobile Internet subscribers. • Implement effective regulation; 2. focus on education and build trusted environment; 3. create positive attitude toward restrictions; 4; control online activity; 5. react promptly. • Self-regulation.
6. Please describe your activities to support online safety	• I am involved in project to implement parental control in JSC SILKNET. • Maintenance of a section on Magticom website dedicated to combating telephony and Internet service fraud. • User management and access policy; penetration testing; implement policies; provide appropriate training; set up and manage firewall; cooperate with governmental agencies and other companies of the industry. • Service contracts, QoS, self-regulation and www.stopline.ge

Question	Responses
7. Provide links to existing published work (e.g. policies, awareness, research, tools, legislation, programmes)	• https://www.magticom.ge/ka/useful-info/fraud-prevention/fraud-news (in Georgian). • Unfortunately, all of works are located on internal network of the company. • Stopline.ge
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	• I am working with our InfoSec team • Magticom is in full compliance of all the existing legal requirements related to online safety imposed by the relevant authorities • Exchange information; provide support if necessary; participate in workshops and training; • MoU with Data exchange Agency- DEA on cooperation on cybersecurity issues and trainings.
9. Can children/parents report online safety concerns or issues to you?	• No • Yes • No • Yes
10. If yes – what sorts of reports do you accept and how can they do this?	• We accept all the reports delivered through current customer interaction channels, i.e. call/contact centre, online support chat etc. • By online request.
11. If no – how can children/ parents report concerns?	• Through company hotline. • Make call on hotline of the company. • Directly to hello@stopline.ge.
12. Describe how you prevent and/or manage online child abuse content?	• We are blocking such websites inside company network. We are blocking websites for our customers, when we receive order from governmental agencies, we do not know if child abuse content are in such orders. • Abusive content is taken down (if our organization is involved in hosting of the relevant content) or the respective web site address is barred from our DNS infrastructure immediately after the relevant report is received, and credibility is established. • Inside the company we restrict different types of web addresses compromised IP's; also restrictions are made based on user's reports and cert.gov.ge recommendations. • Ask for filtering/blocking directly from ISPs.
13. What initiatives or strategies would you like to see to improve online safety?	• More strict law. Increase of public awareness. Block several content. • Development of public registry of abusive web sites, which are required to be taken down and/or disconnected . • Multi Stakeholder approach and self-regulation.

Question	Responses
14. What would you say are three key challenges in the online world?	• Keep people safe. Access to technologies for terrorists. Gather huge power to irresponsible people. • "1. Timely discovery and disclosure of abusive content web sites. • 2. The development of streamlined legal and operational procedures for dealing with abusive/unsafe content. • 3. Complexity and inadequacy of technical capabilities required for enforcement of the content filtering rules and policies" • Facilitates violation of privacy, the commission of a crime and abuse • Censorship and education of parents and kids.
15. What would you say are three key opportunities in the online world?	• education. Access to information for everyone. Create more advanced product and services • "1. Making online world safer will make sure the online content more useful in general • 2. Improved online safety will increase general availability of online content • 3. Increased safety means increased trust in online content " • Increased availability of better education; get quick access to necessary information; better job opportunity • Access to the information and freedom of expression
16. What other comments would you like to make?	• Online services are increasing very fast, fraudsters are more and more advanced. Law enforcements are not so fast and motivated. • Wish you success in your activities endeavour. • We need more self-regulation and have very good examples for cooperation

University

Question	Responses
1. To what extent is online safety and children’s rights your responsibility?	Partly in my responsibilities
2. How is online safety and children’s rights integrated into your existing policies and processes?	In our existing document: "Information technology (IT) management policies and procedures" it is reflected somehow.
3. To what extent is online safety covered within existing legislation?	Partly
4. Which of the following areas do you focus? (Tick all that apply)	Education, Tools and Awareness, Legislation/Policy, Research, Data Protection, Information Security
5. What are your online safety priorities?	Managing Internet Services
6. Please describe your activities to support online safety	Managing Network supervises and regulation

Question	Responses
7. Provide links to existing published work (e.g. policies, awareness, research, tools, legislation, programmes)	
8. With examples, please describe how you work with other agencies and organisations to improve/progress online safety?	
9. Can children/parents report online safety concerns or issues to you?	Don't know
10. If yes – what sorts of reports do you accept and how can they do this?	
11. If no – how can children/ parents report concerns?	
12. Describe how you prevent and/or manage online child abuse content?	
13. What initiatives or strategies would you like to see to improve online safety?	
14. What would you say are three key challenges in the online world?	
15. What would you say are three key opportunities in the online world?	
16. What other comments would you like to make?	

Appendix D: Mission agenda and stakeholder details

Programme of the visit of the experts in Tbilisi and schedule of the expected meetings for preparation the "Safe Internet – National Strategy and its Implementation Action Plan" (22 – 25 October 2018, Tbilisi)

Monday, 22 October

Time	Meeting content	Attendees (Name and Title)
13:00 – 13:30	Meeting with the MoESD Team	
14.00 – 16.00	Introductory workshop with the stakeholders of Safe Internet – NSIAP project in GITA, • Presentation of the challenges and opportunities of Internet Safety; The methodology of elaboration the Safe Internet – National Strategy and its Implementation Action Plan • Brief introduction on their involvement by stakeholders	All Stakeholders
16.00 – 16.30	Coffee Break	
16.30 – 17.00	Discussion and (Q & A session)	
	End of Day 1	

Tuesday, 23 October

Time	Meeting content	Attendees (Name and Title)
10.00 – 11.30	Meeting with the Ministry of Education	Sophie Burduli, Department of Strategic Development, Strategy Planning Division Giorgi Gvasalia, Information Safety Manager, Computer systems, networks and communication Service, EMIS
11.30 – 13.00	Meeting with the Ministry of Justice and the DEA	Nikoloz Gagnidze, Head of Data Exchange Agency Nata Goderdzishvili, Head of Legal Department
13.00 – 15.00	Free time	
15.00 – 16.30	Meeting with the Georgian National Communications Commission	Mariam Sulaberidze, Head of International Relations Department Kety Rekhviashvili, Head of Market Analysis and Strategic Development Department
16.30 – 18.00	Meeting with the Ministry of Health	Sophio Barbakadze, Chief Specialist, Social Defence Department
	End of Day 2	

Wednesday, 24 October

Time	Meeting content	Attendees (Name and Title)
09.30 – 12:30	Meeting with schools and children	Marina Zhgenti, Director, New School Manana Turkadze, Director Galaktion Tabidze Tbilisi Public School №51
12:30 – 14:00	Free time	
14:00 – 15:00	Meeting with the Adviser to Minister of MoESD	Lasha Mikava, Adviser to Minister MoESD Team
15.30 – 17:00	Meeting with the Ministry of Internal Affairs	Ketevan Tatuashvili, MIA, Human Right protection Department Giorgi Revishvili, MIA Giorgi Japaridze, MIA, Cyber Crime Division Sopio Rukhadze, LEPL 112, Analyst Beka Kakheli, LEPL 112, Information Security Manager Sofiko Alaverdashvili, MIA, Information Analysis Department
17:00:18:00	Meeting with NGOs	Transparency International Georgia ISOC Georgia Geo IGF Georgian Suicide Prevention Association
	End of Day 3	

Thursday, 25 October

Time	Meeting content	
10.00 – 11.00	Meeting with telecom operators, TOA	Caucasus Online Magticom SilkNet/Geocell New Net Systemnet Telecom Operators Association (TOA)
11:00 – 12:00	Meeting with Public Defenders Office	Ketevan Sokhadze, Child Rights Center
12:00 – 13:00	Meeting with Office of the Personal Data Protection Inspector	Kety Bojgua, PR Victoria Bundturi, Legal Department Alexandre Mezurnishvili, Information Security Officer
13.00 – 15.00	Meeting with the MoESD Team for sum up the meetings with stakeholders	
	End of Day 4	

Acronyms

CERT	Computer Emergency Response Team
DEA	Data Exchange Agency
GNCC	Georgian National Communication Commission
GRID	Global Resource and Information Directory
GDPR	Global Data Protection Regulation, EU LEX
INHOPE	Is an active and collaborative global network of Hotlines, dealing with illegal content online and committed to stamping out child sexual abuse from the Internet.
INSAFE	European network of awareness centres promoting safer and better usage of the Internet. It is co-funded by the Safer Internet Programme.
ITU	International Telecommunication Union
SID	Safer Internet Day
SWGfL	South West Grid for Learning

International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Office of the Director
Place des Nations
CH-1211 Geneva 20 – Switzerland
Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Deputy to the Director and Director，Administration and Operations Coordination Department (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Infrastructure Enabling Environmnent and e-Applications Department (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Innovation and Partnership Department (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Project Support and Knowledge Management Department (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication Union (ITU)
Regional Office
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

Email: itu-addis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des télécommunications (UIT)
Bureau de zone
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

Email: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication Union (ITU)
Area Office
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de Telecomunicações (UIT)
Regional Office
SAUS Quadra 06, Bloco “E”
11° andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication Union (ITU)
Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Arab States

Egypt

International Telecommunication Union (ITU)
Regional Office
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

Email: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia and the Pacific

Thailand

International Telecommunication Union (ITU)
Regional Office
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

Email: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication Union (ITU)
Area Office
Sapta Pesona Building, 13th floor
JI. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

Email: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

CIS countries

Russian Federation

International Telecommunication Union (ITU)
Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation

Email: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Switzerland

International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Europe Unit (EUR)
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5111

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-28921-8

9 789261 289218

Published in Switzerland
Geneva, 2019

Photo credits: Shutterstock