Comparing Children's E-safety Strategies with Guidelines Offered by Adults

Birgy Lorenz[1], Kaido Kikkas[1,2] and Mart Laanpere[1]
[1] - Institute of Informatics, Tallinn University, Estonia
[2] – Estonian Information Technology College, Estonia
birgy.lorenz@gmail.com
kaido.kikkas@tlu.ee
mart.laanpere@tlu.ee

Abstract: The ways our children are using Internet have changed significantly within the last five years: the Web experience is more personalised, social, open, self-regulated and oriented towards ripping, remixing, sharing, following, reflecting. As a result, also e-learning has recently become more social and open, involving the use of personal learning environments or social networks. We believe that the schools are not ready for this yet, as strategies and regulations supporting open learning are not up to date. It may seem easier to restrict the use of e.g. Twitter or Facebook rather than integrate them into the learning process.

In 2011, we carried out the qualitative analysis of 201 e-safety related short stories presented by students (aged 12 to 16), parents, teachers, school IT managers and police officials, collected through the Safer Internet in Estonia EE SIC campaign. 2/3 of the stories are fictional – they may be based on urban legends which however appear to refer to real stories. 1/3 of the stories reflect real incidents. We mapped typical behaviour patterns and beliefs regarding privacy as well as the regulations and limitations concerning the use of social networks at schools.

Our study shows that typical safety incidents are not solved adequately when existing regulations are used by the schools. We found that most of the solutions used by schools to ensure e-safety are either technical or purely regulation-based, only some schools appeared to have studied or elaborated on pedagogical or behavioural aspects. Problems are defied by limitations and regulations, while actual safety incidents (whether in- or outside school) remain largely unsolved (or even undetected). Thus there is an urgent need for information and working guidance mechanisms for managers, teachers, parents and students. These matters must be solved before schools reach the critical mass in using e-learning, social networks and modern gadgetry as parts of curriculum.

Keywords: online safety, schools, policy, new technologies, social media

1. Introduction

Massive internet repositories and on-line tools have given schools and homes the opportunity to educate children in new ways – we can use digital images, animations, videos, direct messaging, social networking, smartphones etc. Studying the PISA 2009 ICT skills analysis in Estonia, the students' time spent on the Net at home is usually dedicated to chat and leisure rather than education, while at school their use of computers is more or less limited compared to a number of other countries (Lorenz, 2011). Also the EU Kids Online II survey states that the most common risk for students is communicating with strangers online or seeing something that they should not see. The main problem is that most adults are still living in ignorance about what is actually going on in their children's online life – something that kids nowadays call "the real life" (EU Kids online II, 2009). So it raises several issues between adults and teenagers, regarding the concepts of privacy, copyright and identity.
ICT is an important cross-curricular theme in the new national curriculum in Estonia, thus teachers are supposed to favour students' use of technology, not restrict it. But when asked about solutions to the problems, most adults still liked the idea of restricting the network/computer use or introducing a lot of rules (so detailed that nobody would actually be able to comply). Students were more appreciative of cooperation and mutual assistance in case of a safety incident – instead of just dealing out sanctions.
Quite often, the internet safety issues in the context of e-learning are addressed in a simplified, black-and-white manner, using rare cases of criminal privacy violation to scare teachers and parents. We believe that fear is not the best teacher in this domain.

Our goal was to:

- evaluate what kind of e-safety stories are told by students and experts (teachers, it-managers, and police), and how they are related;
- find typical e-safety stories to promote development of regulations in these areas;

Reference this paper as: Lorenz, B., Kikkas, K., and Laanpere, M. "Comparing Children's E-safety Strategies with Guidelines Offered by Adults." The Electronic Journal of e-Learning Volume 10 Issue 3 2012, (pp326-338), available online at www.ejel.org

- analyse the e-safety stories to find out where do students turn for help and what makes them react in case of an incident;
- determine typical solutions used by children and find out how they differ from the 'mainstream' advice offered by adults, media, awareness trainers etc.

The previous studies in this matter can be divided into 6 bigger groups: cyber bullying (Berson 2002); moral issues – pedophilia, inappropriate content, behavioural errors (Akdeniz 1997; Carr 2004; Mitchell 2004; Peters 2009); programs and materials for schools (Wishart 2004); threat analysis for e-learning (Alwy 2010); normal teenage internet usage (Bullen 2000; Enochsson 2005; Dworschak 2010); Internet usage analysis (Livigstone, 2011; Safer internet for children qualitative study in 29 European countries 2007; Towards a safer use of the Internet for children in the EU – a parents' perspective 2008). While according to the EUKids Online II survey (Livingstone 2010), Estonian students are among the top users of Internet and have had substantial exposure to online security risks, there has been next to no attempt of national-level regulation in this field.
The solutions usually prescribed in this area are mostly technical or are as simple as: "stop-block-tell". Blocking is likely not the solution for the students, even if our currently typical awareness training is centred on that. Also, questions rose about understanding the problem and one's responsibility to react. The lack of knowledge about technical solutions seems to be widespread in that area – even things like simple reporting or blocking unwanted picture/video in Facebook/YouTube are often unknown to neither children nor adults.
We analysed the typology and sources of safety incidents, the real solutions offered, the students' thoughts and feelings stemming from the situation, the solutions suggested by students and whether these typical solutions actually apply in real-life situations. The practical experience of students, teachers, IT managers and police indicates a gap between the measures used in education and real life.

2. Background

The EU Kids Online II states that Estonian children are among the top five when it comes to using Internet and online communication, but on the downside they also experience more cyber threats - sexual imagery, bullying, sending/receiving sexual messages, meeting strangers online, data misuse etc (EU Kids online II, 2009).

In comparison, for the e-learning community the online threats are mostly about keeping up the servers, data misuse/theft and sensitive data (Alwi, 2010). The question of privacy has emerged as well (Becta, 2008).

A typical Estonian home offers good opportunities to use technical gadgets and Internet, but at schools, ICT-related activities are not widely used in the classroom yet. The PISA 2009 segments Estonia to the same group with Portugal and Israel, instead of putting us together with our geographical and cultural neighbours - Finland, Sweden, Norway and Denmark (PISA, 2009).

Legally, the regulations and policies at Estonian schools rely on the Penal Code and generic school regulations that differ from school to school. When we studied the development of new regulations focusing on e-safety, we found that Estonian school leaders were not ready to adopt new rules, but they were open to suggestions (especially concerning the problems which were understood to be serious, e.g. cyber bullying, illegal picture/video taking or slandering). Still the problem with detecting e-safety incidents remains – one of the prime reasons being that teachers and students don't discuss the events and many incidents are kept secret (Lorenz et al, 2011).

The awareness training in the e-safety area has become very popular around the world in recent years (a good example is the Insafe campaign), but for Estonia, 2010 was the first year when systematic awareness training was undertaken for parents, teachers and students and related international networks like InHope, Hotline, Helpline were consulted for help (Hallimäe, 2010).

The area of e-safety awareness discusses the balance of both preventive and reactive action on the cases. There is an abundance of awareness-themed material available in English (which is understood by many teachers) but the main problem is in the prevailing mindset among both teachers and parents. They typically only get interested in the situation after either an actual incident or a large-

scale media coverage in that field. A good example is the “Spanish girl” incident involving a Spanish man posing as a girl to Estonian boys; a boy committed suicide after a year of harassment (The Spanish case, 2009).

The new National Curriculum for Primary and Secondary Schools prescribe the use of multitude of digital tools in the learning process: virtual learning environments (VLE), personal learning environments (PLE) and other web 2.0 resources like social networking to be used in a classroom (National Curricula 2010). A recent study shows that even with the good existing training opportunities and guided by the requirements of the new curriculum, most Estonian teachers are not ready to facilitate students in the matters of e-safety (Maadvere 2010).

In the teachers' communities there are some discussions about differences about real life needs of a 21st century learner and how should the schools meet them. There are rising new challenges like the digital divide, being a part of the global internet village, digital sociality, familiarity in communicating; the roles of student and teacher have changed as has the understanding of policies and responsibilities (Veldre 2010, Murumaa 2010).

There are plenty of materials (usually in English) that urge teachers to discuss these matters with students. But they are usually used as a reaction rather than a preventative act. At first, nobody believes it could happen to them; yet if something happens, it's not announced and discussed as people are ashamed (Hoiser 2009).

Teachers are usually reluctant about e-safety - likely most schools have some video posted in the internet featuring a teacher who is unaware that he/she is a 'movie star' or that students secretly film other students (Vasli 2011). Discussing e-safety incidents tends to lead the schools to implementing internet usage restrictions rather than looking for actual solutions. Schools and parents are interested in monitoring child’s behaviour in the name of preventing cyber bullying or meeting strangers (Hunter 2005).

Studying school policies and practices, we could only find technical rules regarding computer wellbeing, time or operational policies (TDL arvutiklasside kasutamise reeglid 2004). Most schools regulate nothing at all, being afraid to create new precedents, or rely on the 'ostrich effect' claiming that having no incidents yet gives them no reason to act. In comparison, British schools opt for much more regulation (Children & Young People's Services 2011). In the United States, similar documents regulating teacher-student relations are given to be signed by both parties (Ohio Policy reference manual 2011).

3. Method

In 2011, we carried out two studies of e-safety stories and bottom-up policy development.
In the first study (Stage I) we used a qualitative case study method and open coding technique (Chamaz 2006).

The aim of the Stage I was to decide who will be the focus group and what are the main topics in the stories. We used the 'go-around' exercise (Fundamental Team and Meeting Skills 2003) with empty cards and clustered the results with 50 participants (10 teachers, 6 experts, others were students aged 12-16). People were divided into 8 groups (6-7 people in the group); 7 groups with students and 1 teacher, 1 group containing teachers and experts) and the goal was to:

- decide who is involved in e-safety incidents and whom children look up to get the information or help from;
- gather and cluster data on what kinds of incidents can usually happen (the overall topics) and what would be important to the community.

The Stage I resulted in 13 different categories to code the e-safety stories.
The Stage II used storytelling as a method. The story is a useful tool for learning - when we analyse stories, we can understand more how the world works for the children (Vilke 2000).

The stories were gathered from the people selected at the Stage I: experts (police officials, teachers, psychologists, ICT experts) and students. The experts were selected from the close group if InSafe

Estonian project using directed focusing (Teddlie 2009). Later we also used the snowball method (Gray 2007) as e-safety educational experts are rare in Estonia. The stories from students were gathered using a storytelling competition at InSafe project workshops in Estonia. We analysed the collected stories in line with qualitative case study method (Gagon 2010).

- 135 students participated in workshop "tell me your e-safety story". We cannot prove them as authentic e-safety stories but we assume that not all of them are myths. These are the stories that parents tell their children and children tell each other.
- 19 stories that children claimed to be real.
- 20 experts' stories were gathered from the interviews or surveys.
- 27 stories by police officials are a representative collection of what they think mostly happens to children that end up reported to the police.

Theexperts presented their stories as situations with solutions.

To code stories we used 13 themes (found in the results). They are more related to human behaviour than is typically discussed in studies about technical e-safety risks in e-learning (Alwy 2010) or e-safety studies like EUKids Online II survey (Livingstone 2010), where the main goal is to address sexual themes. We were more interested in the typical internet/computer interaction experience of an average student. For that we used 180 stories out of 201, as some stories were excluded due to being too short.

In the Stage III of our study, we chose 28 stories about five code groups (cyber bullying, harassment, slandering, fraud and privacy). The stories were selected with the help of the expert group (teachers, ICT experts, police officals and a psychologist) to cover most common cases that have emerged during the recent years. A lot of the stories overlap in coding - a story can be counted to be about privacy, but also about cyber bullying.

We had three groups of surveys and picked different cases from the five coding areas. All in all, 192 students aged 10-16 from 10 different schools (6 city and 4 rural) responded (the complete list of cases can be found at http://tinyurl.com/cpcona6). We proposed ten types of potential strategies for coping with each type of e-safety incidents:

- do nothing;
- find a technical solution myself;
- try to talk to the offender myself;
- block;
- counterattack;
- inform the victim;
- take it as a point to be smarter next time
- like it, will use/copy it myself;
- ask help from informal sources (friends, parents, teachers);
- ask formal help from officials (police, service providers);
- other.

Finally, we interviewed the expert group about their solutions to the cases to compare them to the student's answers.

4. Results

We used an open coding approach to categorise the stories between 13 topics: spam, gaming, computer overuse, virus, fraud, passwords, fake accounts, cyber bullying, harassment, slandering, privacy, pornography and meeting strangers. These were the topics or labels that emerged after reading the stories several times. Every story was then labelled with one topic (primary code), which appeared to be the main focus of this story. Figure 1 illustrates the differences of stories collected from police, experts and children.

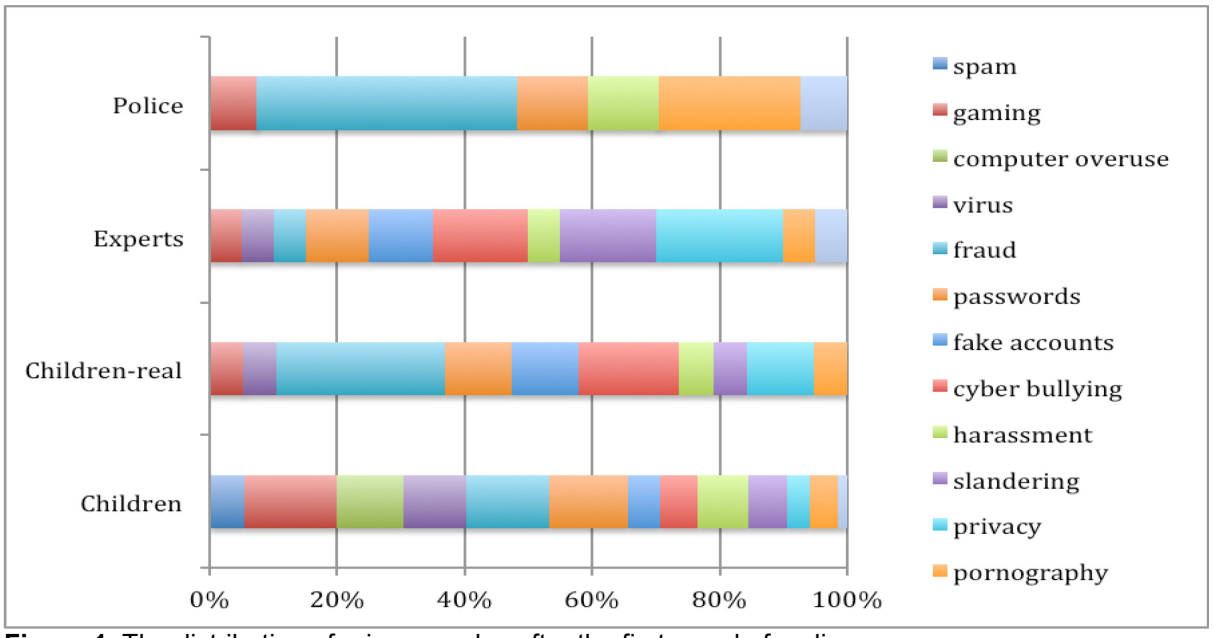

Figure 1. The distribution of primary codes after the first round of coding

As most of the stories actually contained references to multiple aspects and not just to the primary topic, we decided to do the second round of coding so that each story could be assigned multiple secondary codes. Figure 2 illustrates the differences of occurrences of secondary codes in stories collected from police, experts and children.

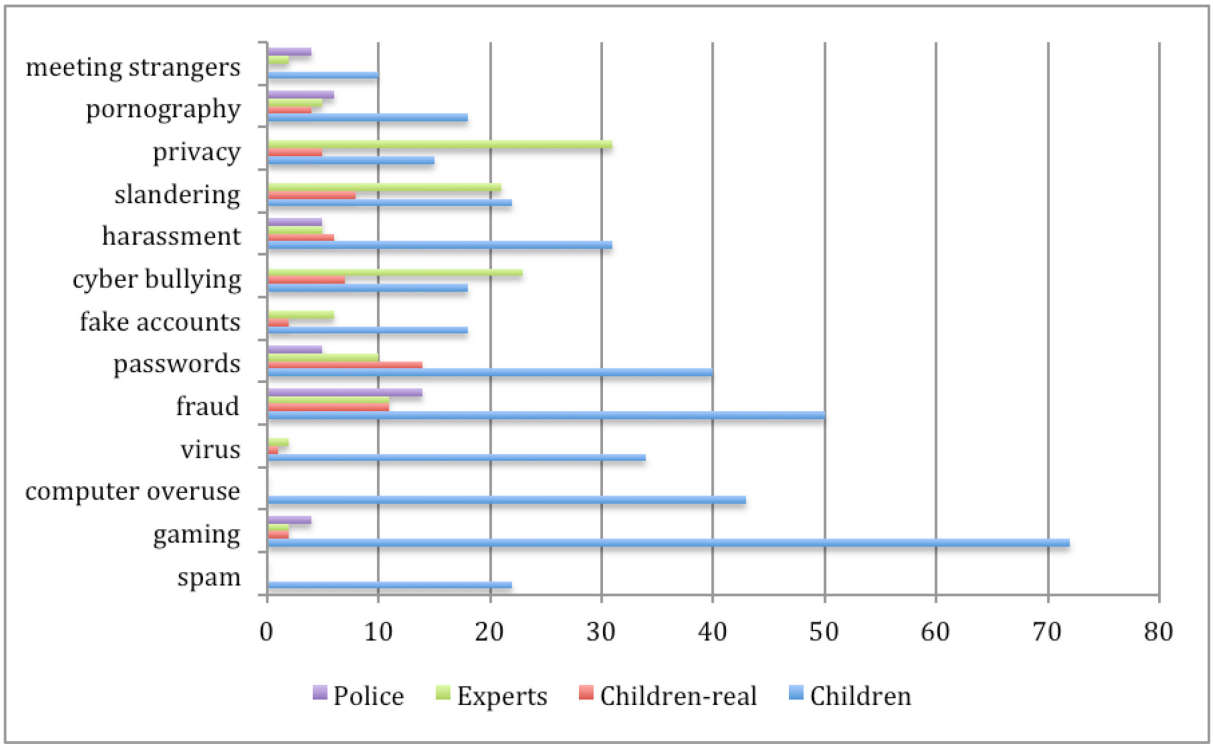

Figure 2. Frequency of secondary codes

Teachers and students present in the interviews some information suggesting that they do not understand what e-safety is about (or there are too many different understandings what is or what is not e-safety) and who is responsible in this matter to help the child.
Teachers claim that

- they have not faced any real e-safety incidents in past 3 years;

- their school is e-safe because their students are not allowed to use WiFi or phones during the school time or they use Web filtering;
- e-safety is a duty for the parents of the students;
- they will create new procedures when something happens.

Students claim that

- they can access internet whenever they want, the filtering of the Web does not work;
- cyber bullying is an everyday act, it can start anywhere and it will not stop when teachers try to stop real-life bullying; sometimes they also punish wrong people.

We also found evidence that the story usually starts with a connection to one environment and changes later; for example, the first connection is established via web or e-mail and afterwards it moves to a social network or a direct messaging system. Most of the connections are made in social networks (Facebook, Rate, Orkut, gaming sites); 90% of the stories took place at home, but schoolmates are usually involved to some extent as well, so we can conclude that the stories are also discussed at school. In comparison with the police stories, the children's stories do not involve mobile phones yet.

The children's stories are mostly about gaming, fraud and passwords. There is a relationship between gaming, computer overuse and viruses, some stories can state relationships between gaming, harassment and pornography. Usually the games are single-player or standalone role-playing games but there was growing evidence about online gaming as well. Fraud has direct relationships to passwords, spam, harassment, slandering and privacy. Fraud is usually seen in the web or social networks, less so in direct messaging. Passwords (scamming, phishing or hacking) are related to web pages, less so to direct messaging or social networking. When we clustered harassment and cyber bullying cases, they can relate to spam, fake accounts and slandering, while harassment is related to gaming, fraud, fake accounts and pornography.

The real cases from children tell us typical stories about fraud, stolen passwords, harassment and slandering. Fraud was mentioned in relation to privacy and pornography. The stolen passwords were mostly related to cyber bullying and slandering. Slandering and harassment were related to privacy infringement, and mentioning of pornography co-occurred with ones of gaming. There were no stories about spam, computer addiction and meeting strangers. There were lots of indications that direct messaging is taking place in social networks or chat rooms and there is no need to add strangers to one's MSN or Skype account- yet that is usually what parents and teachers address in e-safety trainings.

The experts' stories address mainly cyber-bullying, slandering, privacy infringement, less about fraud and stolen passwords. There are direct relationships between privacy and slandering, bullying and passwords. Most stories are related to networking or using web.

The police stories show us what kind of help parents need from the legal system. They are usually related to fraud and pornography, less related to passwords, harassment and meeting strangers. There are some relationships between gaming and passwords; harassment and pornography, meeting strangers and pornography. Fraud is usually related to mobile phone or is carried out by mobile phones. Typically, parents turn to police when they have lost money. The police cannot usually interfere when there are moral problems only. There are some relationships between direct messaging, pornography and meeting strangers because in direct messaging one can use video transfer.

The stories from police indicated which paragraphs in the Estonian Penal Code are applicable for internet crimes: PenC § 179 for showing pornography to minors, PenC § 217 for password hacking, PenC § 157-2 for identity theft, PenC § 213 for other computer frauds (Penal Code 2002).

Our analysis of e-safety policies found on the official Web sites of ten Estonian secondary schools revealed that many schools address e-safety issues not with policy measures, but with technical access restrictions, e.g. filtering some web sites or blocking some services. Only a small number of

schools had e-safety policies, which addressed topics like cyber bullying or sexting (sending sexual texts or images by mobile phone). Some schools had regulations on taking pictures in school premises or sharing the visual material originating from the school (see Table 1). The government does not impose any relevant regulations on schools, besides generic legislation (e.g. penal code). While there are regulations used to develop school internal rules, they contain no mention of e-safety. Moreover, while schools are subjected to Lesser ISKE (Estonian three-level IT baseline protection system) framework, no practical support is provided.

Table 1: Typical school rules regarding to use of ICT (based on policies of 10 schools)

Type	**Rules**
Technical	Every class or user has got a different account The right to install or run software or print files is restricted or limited Technical filtering of the web
People	There are goals and priorities of the tasks what you can do with the school computers There are rules regarding the use of social networking sites and direct messaging Computer lab working hours and health related rules (how long can you use a computer) are set Physical well-being of the computer workstation Monitoring students gaming is usually not allowed
Other	Penalties for breaking the rules Information where to turn for help One can suggest ideas

We also found indications about what kind of regulations are needed. The common recommendations were the following: the school must be present in the network because it motivates students to behave better; the school must develop rules regarding mobile and other devices' use in school premises; the school must filter programs and the web in computer classes; students should pledge not to make fake accounts or post in somebody else's name; students should pledge not to share his/her passwords with others; students should pledge not to slander others on the Net; students should pledge to ask permission from other people before taking pictures in the school premises.

The students considered the most important stories to be the harassment case involving a younger sister, who was asked to share webcam sex with a stranger; the privacy story about the party pictures from the previous day were uploaded to Facebook; the story about intimate pictures which were uploaded to the Facebook by a boy after breaking up with his girlfriend; the fraud case where a mobile phone was used to extract money from the victim and also a case about buying goods online.

The topics that were given the most "other" answers were about how to react on the harassment case; a slandering case where a mother found out that her son has made a web community named "Naked butts"; a cyber bullying case where a boy made a secret account for the principal and posted humorous stories there; a case of someone having deleted all other students files from the class computer; a fraud case involving plagiarism (students were buying reports from the net); a case of someone taking a school band song and presenting it to the Eurovision Song Contest without their consent, and the last one was about buying a hairdryer from the net and getting nothing.

The solutions offered for different cases seem to reflect the lack of knowledge (awareness) and regulations in these areas. In some cases there was also disagreement between experts (teachers and police) about what is the right solution, like when to react, how to react and what is one's responsibility to act. Police was more eager to rely purely on law, while teachers were more apt to decline to follow it literally as it was considered not educational to run to police every time when some prank was done by the students.
We distributed the cases into two (real and Net life problems and only Net related problems) and by topic into four categories by coding privacy, slandering, fraud, and cyber bullying or harassment (see Figure 3).

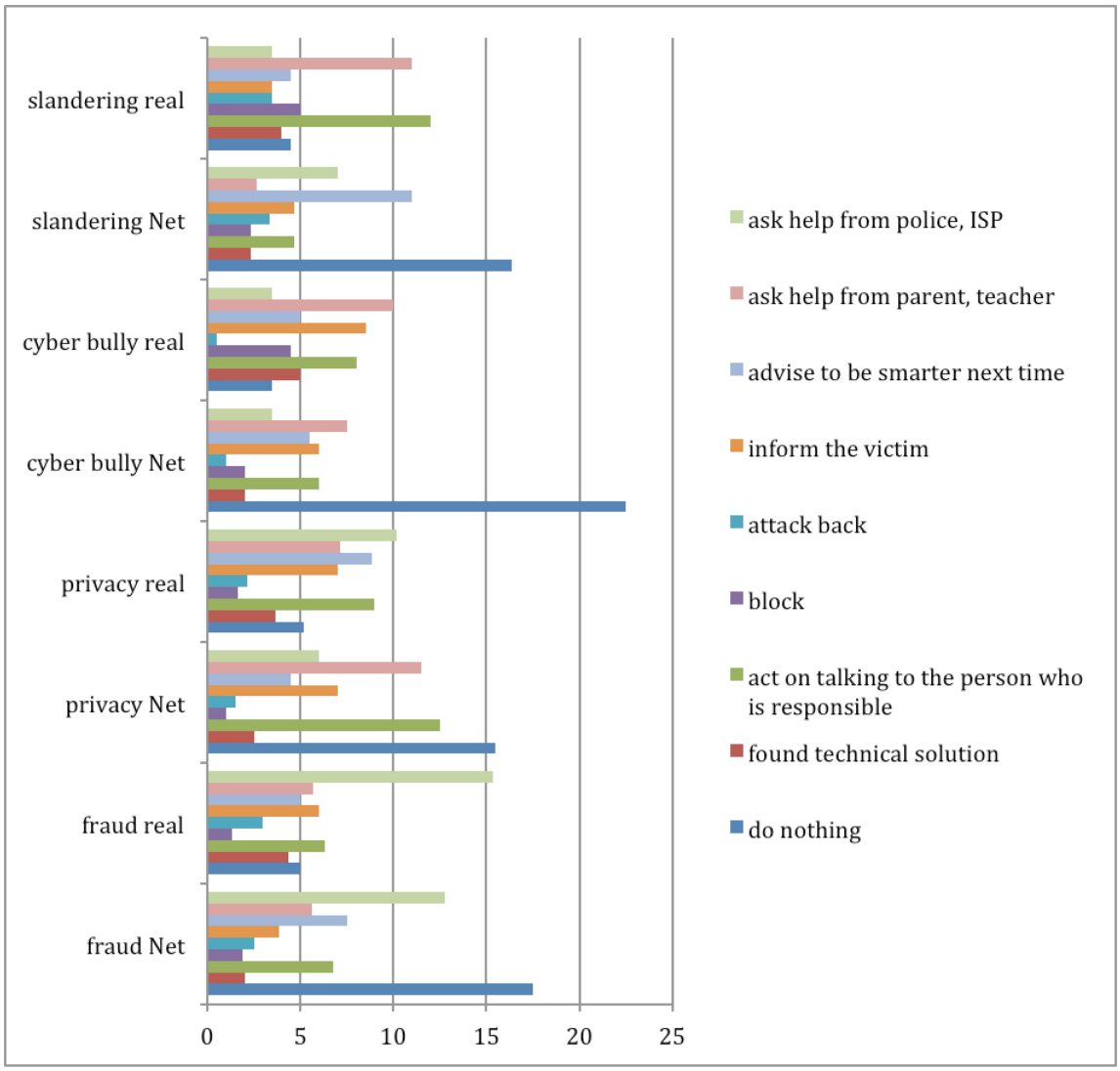

Figure 3. Children's preferred e-safety strategies

We also interviewed experts regarding their preferred solutions to the same problems. Results of the interviews are compared with the preferences of children in Table 2 below.

Table 2. The guidelines offered by adult experts in comparison with the preferred strategies of children

Topic	Adults (experts and teachers)	Children
Privacy violation	Raising awareness, changing one's settings, knowing better next time, responsibility to give advice. Depending on the case one should turn to the ISP, website owner or police.	The person's own problem; no explicit way to react, depends on the case.
Fraud	Turning to police or ICT expert for help, no reaction or ignoring (teachers).	Turning to police in some cases (only when there is direct money loss), no reaction in cases of fake accounts and hacking.
Cyber-bullying and harass-ment	Obligation to react and seek for help, blocking, announcing the incident, evidence gathering. Recommended to seek out trusted adults, teachers or police.	Mostly ignoring. Some other cases involve seeking help, informing the victim or taking initiative (counter-attack).
Slander	Reporting to the service provider, asking to remove the information.	Mostly ignoring. Some cases involve informing the victim.

As a summary, some general inferences can be made from our data analysis:

- students lack knowledge about where to look for help when something happens. There is a question whether to react at all, as a lot of e-safety cases are typically ignored;
- students tend to seek out the informal help (friends, family) who may turn out to be even less knowledgeable;
- the reputation of police is also high, as seen in several cases - but sometimes the police does not have the power to help, because there is no direct money loss or the legislation is ineffective or lacking;
- on student pranks aimed to teachers, the suggested solutions differ – sometimes they inform the teacher, but usually they don't. When other children are involved in the case, they usually say "it is your own fault – be smarter next time".
- students make distinction between school and personal problems – a school problem is something that school should deal with (even e.g. when someone of the students themselves deleted other another student's files). A personal problem sometimes ends up in the victim counterattacking the bully (e.g. somebody's account is hacked or illegally used, the victim can seek vigilante justice).
- when there is a case about leaking private data, students tend to also utter "be smarter next time", because they might interpret it as already common knowledge. For most of them, private data is phone numbers or home addresses, not pictures and videos;
- students lack technical knowledge about how to block, report or gather evidence when using social networking tools. It seems to be selective - when some newspaper or advertising company tries to exploit the situation they know their right to seek help (usually police);
- students try to find solutions themselves rather than get adults involved - even in the situations where the correct way would be to turn directly to the police (identity theft, hacking or illegal entry to another person's account);
- when somebody is being directly harassed, the students will react - they seek help from police, parents or teachers. This is the only case when they do not ignore the problem;
- when there is direct money loss involved (usually phone-related cases), students will turn to the police. But when there is just money-making involved (like in the case where a boy tried to sell his account for money), they think it as a personal matter;
- analysing the "other" eg. "k" answers, we found a lot of implications to violence - such as in the cases where the wrongdoer is somehow known to the victim. In these cases, some victims would attempt to deal with the bully in real life or start bullying others in turn.
-

Often, schools do excuse their unawareness with „we'll react when it happens"(secretly believing that it will not happen). Most schools also try to delegate such problems to parents - who in turn look up on schools for help, as their only reaction to safety incidents is often to apply time limits on Internet use. We found that students tended to choose stories about illegal picture/video taking, fake accounts (identity theft) or hacking MSN/Facebook accounts. At the same time, teachers are more worried about situations like "students are spreading teacher's picture on Facebook". Students are more tech-savvy which in turn can lead into some unpleasant consequences like plagiarism or disregarding copyright. Schools are expected to apply new technologies in teaching and learning, but safety of student and teachers is paramount in this context.

5. Discussion

The analysis of the students' e-safety stories revealed several issues. It is clear that many students don't apparently understand what e-safety means. Usually, students do not think that they are in any way involved in an e-safety incident, even if they have been harassed or bullied on the internet e.g. in a YouTube video about the teacher. Gathering stories from the "storytelling'" exercise and from the web-based competition give similar results. Also when we did a test with a control group giving students an e-safety topic to write about, like privacy or viruses, they would rather write something to please us and later change the story to somethingthat they actually wanted to write about. It was quite

interesting that they were not thinking about the given topic but rather writing about their real problems. It is something we should study further on in a deeper level.

The students' stories are highlighting the privacy issues in the social networks as it is easy to create fake accounts, gather personal information from search engines or even take pictures with mobile phones and post them. Instead, people tend to believe that privacy is someone else's problem. Also, they often state that it's difficult or they don't have time to change privacy settings, but after an incident they suddenly start to believe that they could learn to do that.

The children's stories do not include stories about pedophilia and meeting strangers that usually are considered to be the biggest threat regarding e-safety. Children do not understand the differences between harassment and cyber-bullying – these terms are foggy to them. It can point to weak sexual education in Estonian schools because in only 4 times out of 17 cases about harassment did they see sexual topics. But it can also be a topic that is not openly discussed among students. Also, the line between privacy and personal data protection is not really understandable to students. Usually, they prefer black-and-white solutions: it's all private or nothing is.

The stories collected from the police and IT experts differ because police officials deal with these stories mostly only when there is a direct money loss. Schools often prefer to deal with the incidents secretly, finding a solution between the parties.

Looking at the results from the e-safety related policies of schools, we found that even when we did present typical sex-related stories to be discussed they were not considered a priority issue for schools. Harsh E-safety regulations at school could (in the eyes of principals) be one of the further reasons for teachers not to use VLE, PLE and m-learning with students and only keep using the teacher's computer and projector for presenting their own materials, which are considered safe.

Although our study focused on analysing e-safety incidents, it also informs the e-learning community about the need to raise awareness among teachers and students about potential threats to their privacy. This need becomes even more evident in the light of new trends related to the use of social media (blogs, wikis and social networking sites) as a new type of online learning environment (Becta 2008).

Another very interesting finding is that while e-safety trainings usually address MSN conversations and stranger issues (with the handy solution of blocking the unpleasant person), the interaction of today has moved to social networks where there is also opportunity to chat. When a child feels the pressure to have more friends than other people then blocking unpleasant persons is not really an option. This creates a privacy problem as well as the child opens his/her life to strangers even without any direct communication.

The main problems that rose from this study confirmed our presumption that the overall understanding of e-safety is weak. It is hard to understand and its reflections in real life are hard to notice. Neither teachers nor police officials can usually be found in the same online spaces with students, so it is getting harder for them to understand the problems that students are facing. For now, Estonian students are using two main social networks – the international Facebook and the local Rate.ee, but if Facebook does not provide protection personal data (or even, as sometimes suggested, is selling it for profit), the students may find another network soon, where there is less adult supervision.

There is also a problem with students' passivity in case of an incident. Is there a need for more awareness training or is it something that they have picked up from the adults? Some adults do also turn away when they see something unpleasant happening ("you see, but you don't really see"). So how to teach students to react when some of the adults do the opposite?

Most of the e-safety awareness trainings tend to offer the guidelines in the style of rule-of-thumb, e.g. "stop-block-tell" or "don't click everywhere". Yet, these guidelines are something that students know but tend to never use. The "click everywhere" mentality leads to computers becoming so full of junk that it is easier to just reinstall the system (typically, students either don't have much local data or they backup it to the clouds). The understanding to keep one's computer up-to-date is rather weak, because even adults tend to consider it someone else's problem - they don't understand that their

computer can become a direct source of a wide variety of problems (illegal data storage, spam distributor, attack springboard etc).

The “Stop-block-tell” solution is something that threatens the person’s fame – to have just one friend or contact less than one's friends is not an option. Also, there is a belief that the net is anonymous and nobody can track one's activities. It was rather surprising that students are usually unaware of the technical defence measures provided by social networks (e.g. report the offending video or picture).
The last but not the least, we were surprised to find traces of real violence that can follow when someone is stressed after an online incident. The outburst will come – it may take different forms like cyber bullying others in turn or doing a nasty prank to teachers. If adults really want to help the child in need, they need to uncover many different layers of the problem before reaching the core. Teachers may often find out that the bully is someone who has been bullied him/herself before. Regrettably, many adults do not usually have time to really go to the roots of the issue – they would rather want to make the problem go away as fast as possible. This will result the children facing the problems alone, being forced to develop their own strategies. Even if for now, there seem to be no universal strategies used by students other than “don’t care about the problem”, this is not an acceptable solution.

6. Conclusion

Our overall conclusion is that typical e-safety policies must stress topics that all stakeholder groups agree being important: gaming, fraud, password, harassment, pornography and meeting strangers. There are direct relations between gaming and passwords; fraud and privacy in social networks; passwords and slandering in social networks; harassment and pornography. Students also point out problems regarding viruses, fake accounts, cyber-bullying, slandering – these are topics at which police is usually powerless to help.

Our analysis shows that only a few schools have explicit policies which target e-safety issues. Yet, even these few existing school-level policy documents fail to address the topics which were most frequently mentioned in the stories written by students.

Next, we should turn our attention towards evaluating the e-safety risks by themselves and how the risky behaviour has changed online learning activities. If Internet use has changed children’s values and patterns of online behaviours then the question is how we as parents and educators can adjust children's behaviour on the net when we still live in a different e-world. We should acknowledge that although we use mostly the same digital tools as the new generation, we still identify and handle the threats related with our online activities in a different manner.

It is easy to say that e-safety is someone else’s problem, be it ICT teachers, parents, awareness centres, police etc - but it is actually everyone’s problem. The solutions offered by many adults differ from the ones offered by students because they don’t understand the core issue – these children actually live in the Net and therefore this is real life for them.

The awareness training about “stop-block-tell” does not work as it is something fundamentally different from how our children are thinking and acting. There is a serious lack of noticing the problem and reacting on it – it is similar to real life, but on the Net, it is just easier to ignore (one just need to close his/her web browser or shut down the computer).

The solution is to include more technical and other practical aspects in the awareness training and distribute step-by-step, common-language how-to-s like how to set one's privacy settings, how to report a page, picture, video or how to behave when someone is being bullied, or what to do when one becomes a victim of fraud or slander. The awareness in these areas is also needed for the adults who are setting the standard how their students or children behave and deal with the problems in the future.

But the question remains - is the “no action” strategy or ignoring the problem common to only Estonian children or is it something that teachers and parents from other countries are also experiencing?

References

Becta (2008) *Analysis of emerging trends affecting the use of technology in education*, Research to support the delivery and development of Harnessing Technology: Next Generation Learning 2008–14

Berson, I., Berson, M. and Ferron, J. (2002) *Emerging risks of violence in the digital age: lessons for educators from an online study of adolescent girls in the United States*, Meridian: A Middle School Computer Technologies Journal Vol. 5 No. 2, NC State University, Raleigh, NC

Akdeniz, Y. (1997) *The Regulation of Pornography and Child Pornography on the Internet*, The Journal of Information, Law and Technology (JILT), UK

Alwy, N. and Fan, I. (2010) *Threat analysis for e-learning*, Int. J. Technology Enhanced Learning Vol. 2 No 4, UK

Bullen, P. (2000) *The Internet: its effects on safety and behaviour implications for adolescents*, Department of Psychology University of Auckland, Netsafe, New Zealand

Carr, J. (2004) *Child abuse, child pornography and the internet*, ISBN 0900984805, NCH, London

Chamaz, K. (2006) *Constructing grounded theory: a practical guide through qualitative analysis,* SAGE Publ. London, GB

Children & Young People's Services (2011) *Internet safety and model policies on the acceptable use of the internet for schools* [online] http://www.bristol-cyps.org.uk/services/ict/acceptable.html

Dworschak, M. (2010) *The Internet Generation Prefers the Real World*, Spiegel Online Internetional

Enochsson, A. (2005) *A gender perspective on Internet use – Consequences for information seeking on the net*, Information Research, 10(4) p. 237

EU Kids Online II 2009 [WWW] retrieved 12.10.2011 http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/home.aspx

Fundamental Team and Meeting Skills: Tools and Techniques (2003) New York State Governor's Office of Employee Relations [online] http://www.goer.state.ny.us/Training_Development/Online_Learning/FTMS/300s4.html

Gagon, Y.(2010) *The Case Study Research Method: practical Handbook,* Presses de Universitete du Quebee, Canada

Gray, P., Williamson , J., Karp, D. and Dalphin, J. (2007) *The Research Imagination: an introduction to quantitative and qualitative methods*, Cambridge University Press, GB

Hallimäe, M (2010) *About Safer Internet in Estonia EE SIC project* [WWW] retrieved 10.11. 011 http://www.targaltinternetis.ee/projektist/?lang=en

Hoiser, F. (2009) *Countering "it won't happen to me",* Safety News Alert [online] http://www.safetynewsalert.com/countering-it-wont-happen-to-me/

Hunter, N. (2005) *"Jenny´s Story" – An internet safety resource developed to combat child abuse on the internet,* Lancashire Constabulary, Pretton, UK [online] http://www.popcenter.org/library/awards/goldstein/2005/05-06.pdf

Linstone, H. A., Turoff, M. and Helmer, O. (2002) *The Delphi Method - Techniques and Applications*, Murray Turoff and Harold A. Linstone.

Livingstone, S., Haddon, L., Görzing, A., & Olaffson, K. (2010) *Risks ans Safety on the Internet: The perspective of European children*. London: LSE: EU Kids Online.

Lorenz, B. (2011) *Eesti õpilaste PISA 2009 IKT-alased küsimuste vastused vihjavad kasutamata ressurssidele koolides.* In National Exam and Qualificaton Centre Pisa Research results page [online]: http://uuringud.ekk.edu.ee/fileadmin/user_upload/documents/PISA2009_IKT_analyys.PDF

Lorenz, Birgy; Kikkas, Kaido; Laanpere, Mart (2011). *Bottom-Up Development of E-Safety Policy for Estonian Schools*. 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV2011), 26.-28.September 2011, Tallinn, Estonia. (Toim.) Estevez, E., Janssen, M.. ICEGOV '11, September 26 - 28 2011, Tallinn, Estonia: ACM, 2011, (ACM International Conference Proceedings Series), 309 - 312.

Lorenz, Birgy; Kikkas, Kaido;Laanpere, Mart (2011). *Social Networks, E-learning and Internet Safety: Analysing the Stories of Students*. In: Proceedings of the 10th European Conference on e-Learning ECEL-2011: 10th European Conference on e-Learning ECEL-2011 Brighton, UK 10-11 November 2011. Academic Publishers, 2011. pp 416-422

Maadvere, I. (2010) *IKT uues põhikooli riiklikus õppekavas* [online] http://tiigrihypeharidustehnoloog.blogspot.com/2010/06/uusoppekava2.html

Mitchell, K., Finkelhor, D. and Wolak, J. (2004) *Victimization of Youths on the Internet*, Victimization of Children: Emerging Issues (pp 1-39) New York: The Haworth Maltreatment and Trauma Press, NY

Murumaa, M. (2011) *Digisotsiaalsus õpetaja ja õpilase suhetes*, Õpetajate leht Vol. 16 [online] http://www.opleht.ee/?archive_mode=article&articleid=5367

National Currcula - *Põhikooli Riiklik õppekava* (2010), Riigiteataja [online] https://www.riigiteataja.ee/akt/13273133

Ohio policy reference manual (2011) *Sample Regulation computer/Online services* [online] http://www.ohioattorneygeneral.gov/getattachment/48c7a1bc-6ccc-4486-8c79-9190f9a3f97a/Teacher-student-relations-sample-policy-for-accept.aspx

Okoli, C. and Pawlowski, S. D. (2004) *The Delphi method as a research tool: an example, design considerations and applications*, Information & Management Vol. 42 pp.15–29

Penal Code - *Karistusseadustik* (2002) Riigiteataja [online] https://www.riigiteataja.ee/akt/184411

Peters, R. (2009) *How Adult Pornography Contributes To Sexual Exploitation of Children*, [online] http://www.obscenitycrimes.org/news/HowAdultPornographyHarmsChildren.pdf

Pisa 2009 Results: Students On Line Digital Technologies and performance vol. 6 [WWW] retrieved 3.09. 2011 http://www.oecd.org/dataoecd/46/55/48270093.pdf

Rubtsova, P. (2011) *Privacy in Social Media*, Tallinn University research

Safer internet for children qualitative study in 29 european countries, summary report (2007) Eurobarometer, [online] http://www.internetsafety.ie/website/ois/oisweb.nsf/0/F7650C73182B83B6802574D5004A932B/$File/Safer%20Internet%20for%20Children-%20Summary%20Report-march-may07.pdf

Spanish case (2009) Anatomy of a series of harassment: how to fool the teen boys (EST) Sariahistamise anatoomia: kuidas kümned poisid lolliks tehti [WWW] retrieved 5.08.2011 http://etv.err.ee/index.php?0554837

TDL arvutiklasside kasutamise reeglid (2004) Tartu Descartes'i Lütseum [online] http://portal.tdl.ee/index.php?module=pagemaster&PAGE_user_op=view_page&PAGE_id=45&MMN_position=65:59

Teddlie, C. and Tshakkori, A. (2009) *Foundations of Mixed Methods Research: integrating Quatitative and Qualitative approaches in the social behavioural sciences*, SAGE Publ. London, GB

Towards a safer use of the Internet for children in the EU – a parents' perspective Analytical report (2008) Eurobarometer, [online] http://www.internetsafety.ie/Website/OIS/OISWeb.nsf/page/DPCY-7MELY61694917-en/$File/Eurobarometer%20Survey%202008.pdf

Vasli, K. (2011) *Sotsiaalmeedia imed: 11 aastat vana raadionalja "Jah narkootikumidele" taassünd,* Õhtuleht Online [online] http://www.ohtuleht.ee/427422

Veldre, A. (2011) *Kohutavate muutuste anatoomia*, Õpetajate leht Vol. 16 [online] http://www.opleht.ee/?archive_mode=article&articleid=5368

Vilke, M. (2000) *Research study on children's story-telling,* Psycholinguistics on the Threshold of the Year 2000, pp. 453-461. Porto: Faculdade de Letras da Universidade do Porto.

Wishart, J. (2004) *Internet safety in emerging educational contexts*, Computers & Education archive Vol. 43 No. 1-2, August 2004 Elsevier Science Ltd. Oxford, UK, UK

