CyberAdventure

FRAMEWORK FOR KEY CYBER SAFETY COMPETENCES

JUNE 2020

Co-funded by the
Erasmus+ Programme
of the European Union

CyberAdventure – Increasing the Cyber Safety culture of children through gaming is a project co-financed by the Erasmus+ Programme, under the Key Activity 2 – Cooperation for innovation and the exchange of good practices for school education

Project no. 2019-1-UK01-KA201

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

EXECUTIVE SUMMARY

The *Framework for the Key Cybersafety Competences* is the first significant deliverable of the CyberAdventure Project. The core aim of the Project is the design and implementation of an innovative computer learning game on Internet Safety to educate children (7-12 years old), that can be easily implemented in formal, non-formal and informal education settings. This deliverable is the outcome of literature research aimed at identifying the most significant competences for cyber safety Education, allowing the consortium to select those which can be better addressed via the final product (the CyberAdventure game).

During the kick-off meeting the partners exchanged information and ideas regarding this issue. Aston, as the leading partner of the corresponding task, undertook the responsibility to conduct a literature review in order to clarify the necessary terminology, but also to examine the state of the art in cyber safety Education in the EU and attempt to propose a framework for the key competences. All partners contributed with data and information about benchmarking tools for measuring such competences. The ADV and BOON members undertook the role of the critical reviewer in order to ensure the quality of the deliverable.

This deliverable comprises of five sections, namely chapters 1 to 4 and one Appendix. In the first section (‘Internet and Children Safeguarding in the Digital Age’), a theoretical background is established, and the necessary terms are discussed, explained and eventually clarified. In the second section (‘Internet Safety Education in the EU’), the cyber Education approaches in the EU Member States are recorded and discussed upon. In section three (‘Defining Cyber Education and Competences’), cyber education and associated competences are defined. In section four (‘The CyberAdventure Education Framework’), the proposed framework is presented, constituting the basis for the future tasks of the Project. Finally, Appendix A (‘Cyber Skills Benchmarking Tools’) provides information about benchmarking tools for measuring cyber safety competences.

ACKNOWLEDGMENTS

We acknowledge the support and funding provided by the European Commission for this research project.

In addition, we gratefully acknowledge the contribution from the CyberAdventure research team members:

O1/A1 - Framework for the key Citizenship

Main authors

UK	Vladlena Benson	Aston University

Partners - Contributors

UK	Anne Edwards	SATRO (UK)
UK	Masha Garibyan	Aston University (UK)
ES	María José Rivera Toimil, Nuria Olga Léon Tobajas	CEIPSO Maestro Rodrigo (Spain)
LT	Indrė Mackevičiūtė	UAB Karalienes Mortos mokykla (Lithuania)
PT	Gonçalo Meireles	Advancis (Portugal)

Partners – Critical reviewers

		Advancis (Portugal)
		Boon (Portugal)
		UAB Karalienes Mortos mokykla (Lithuania)
		Aston University (UK)

Table of Contents

Co-funded by the
Erasmus+ Programme
of the European Union

INTRODUCTION

One out of three internet users is a child. They go online at an ever-younger age and they tend to spend an increasing amount of time on the Internet (European Commission, 2007a). It is believed that in Europe today, children on average start using the internet when they are 7 years old (European Parliament, 2018). They spend more time on the internet and social media, play more online games and use mobile apps, frequently without supervision by adults (European Commission, 2009).

While the internet offers many opportunities for learning, communication, creativity and entertainment, it also opens up certain risks to vulnerable users, such as children (European Commission, 2019). This is where Online Safety Education can make a difference, by empowering and protecting children against Internet risks. The Online Safety Education has been a priority for the EC for the past few decades. The EC established the Safer Internet Programme, followed by other programmes, namely the current European Strategy for a Better Internet for Children COM(2012) (European Commission, 2012).

According to this strategy, Online Safety Education should begin early on, when children start having regular contact with the Internet. In particular, by raising the awareness of the Internet risks and promoting responsible behaviours online, the project is equipping children, but also educators, with basic skills and key competences that help them to develop their digital skills and media literacy, thus improving their job perspectives and employability as well as helping them become confident digital citizens (European Commission, 2012; EEAS, 2019). In a recent study conducted in the UK – the Global Teachers Survey (The Royal Society, 2017) – 99% of teachers argued in favour of having online safety education as part of the school curriculum from the age of 7. Teachers have, in this context, an important role to play. They are in contact with the children’s social dynamics, and they often witness first-hand the internet risks. In fact, the Global Teachers Survey (The Royal Society, 2017) reveals that 37% of teachers have already witnessed an online safety incident in their classrooms (sharing personal information or cyberbullying, for example). The question that inevitably follows is whether teachers are equipped to address online safety topics in class. Evidence says that in most cases teachers miss the competences and the resources to do it, limiting their power and their will to act. This is what the Global Teachers Survey (The Royal Society, 2017) also highlights, as 82% of teachers said they didn't feel they had the necessary resources to teach online safety to their students.

The response to the need of addressing Online Safety early on in school and equipping teachers with the resources to do it, is to provide teachers with an easy-to-use learning tool that can help overcome their lack of competences regarding online safety topics and engage children in the learning process.

INTERNET AND CHILDREN SAFEGUARDING IN THE DIGITAL AGE

Online Safety Education encompasses a wide set of skills and knowledge that are widely recognized as essential in an ever more digital world when the social distancing strategies are relying on the internet technologies.

Online trends

Due to COVID-19, most EU countries have been implementing national lockdown measures, such as social distancing, public event cancellation and school closures. Prolonged school closures may have profound negative consequences for young people, both academically and in terms of their mental well-being. One valuable way for pupils to avoid the negative impacts of isolation is to communicate with friends online, but increased time online brings its own risks. We are aware that the constantly evolving cyberworld that children inhabit can easily leave parents one step behind, with emerging trends such as Houseparty, Steam and Zoom being reported nationally as potential concerns. Parents are encouraged to have an open conversation with their son or daughter about their online presence and behaviour and the steps they are taking to protect themselves. Whilst they are often a step ahead in terms of the apps and sites they are using, they don't always consider the need to protect their personal information and avoid potentially negative interactions with others.

Health and Wellbeing

Schools are very aware of the need to help pupils protect their mental wellbeing during the ongoing lockdown and this is supported by the structured programme, which has been altered to focus on staying mentally healthy through online resources. There is an array of resources for parents and young people, such as the YoungMinds website[1] for any pupil or parent looking for advice.

[1] https://youngminds.org.uk/

INTERNET SAFETY EDUCATION IN THE EU

Cyber safety education concerns the provision of a variety of skills, knowledge and attitudes that are central to developing an internet-safe culture and also shape the mind-sets of young people.

States have yet to develop a common policy or a strategic approach to cyber safety education or a common cyber curriculum and teaching methods; whereas not all teachers and education leaders in Europe are sufficiently trained in internet and ICT education - a set of transversal key competences for personal and professional purposes (European Parliament, 2015).

Partners carried out extensive research on studies and reports, particularly those produced by the EU on online safety, cyber security and digital citizenship. This research was important to validate the opportunity to develop the project, as well as to establish the project's scope. These documents included:

- European Strategy for a Better Internet for Children COM(2012) 196 final (European Commission, 2012)
- EU Child Safety Online Project, EC (European Commission, 2018a)
- Alliance to better protect minors online, EC (European Commission, 2018b)
- The European Union Agency for Fundamental Rights (FRA, 2018)
- Self-regulation for a Better Internet for Kids (European Commission, 2018c)
- Key priorities of the EU e-Skills strategy - 'e-Skills for the 21st century' COM(2007) (European Commission, 2007b)
- Protecting Children in the Digital World COM (European Commission et al, 2011)
- European Framework for Safer Mobile Use by Younger Teenagers and Children (European Commission, 2007a)
- Children and Parents: Media Use and Attitudes Report (OFCOM, 2019)
- Global Teachers Survey (The Royal Society, 2017)

Internet Safety Education in Spain

The Internet and social networks have experienced unprecedented progress in recent years and have become the most widely used means of communication by society. The ease of use and dissemination exposes citizens to multiple risks that affect their privacy and rights.

Among young students, the use of computers and smart phones is practically universal (95.6%, 91% at 12 years old), while 87.1% use the Internet. This easy access and familiarity with the use of new media exposes them to a series of risks over which they have not always received sufficient training. They are not fully aware of the personal and legal consequences that may arise from certain practices, and do not take into consideration the fact that any information that is made available to a third party, due to the ease of the means, may end up being used in a totally different context, even to harm others or themselves.

To protect users of these media, especially minors, Spanish government has launched multiple initiatives to inform and raise awareness of the risks associated with their inappropriate use, offering resources that help protect their personal information and their digital rights.

Spanish Organic Law 3/2018, of December 5 (Ley Orgánica 3/2018) *on the protection of personal data and guarantee of digital right* - has been an important step forward by including the right to digital education as an instrument of learning and acquisition of the skills and abilities necessary for the development of minors in the digital environment.

In order to protect young people, help families and schools and to promote and support the development of digital education, and as a result of the collaboration of several institutions and entities, public and private, the Ministry of Education has launched the Organic Law 3/2019 regulation (Ley Orgánica 3/2019), as well as special websites, that is addressed to young people, teachers and families and which purposes are:

- To teach students how to use the internet safely.
- To protect young people while using the internet.
- To help families and schools with dealing with the internet and the use of it by young people.
- To promote and support the development of digital education of young students.

These are some of the resources that the Ministry of Education has launched for students:

- A test[2] to do online and know the starting point for young people.
- **Selfie seguro/Safe Selfie[3]**. Ten situations to avoid a dangerous selfie

  Many people die every year while taking a dangerous ‘selfie’. Although this doesn’t always end in a disaster, selfies are often taken recklessly, driven by the desire for social media publicity or participating in a CHALLENGE.

  It is not only the ones who star in the image who may suffer some serious damage, other people and their PRIVACY may also be affected, as well as (although this is less common) objects of great artistic value.

  Through a series of funny videos and posters, students are made aware of the risks of a dangerous selfie.

- The GAME Pandijuegos[4]. Through animated characters, students have at their disposal a series of games that teach how to protect your identity and make a positive and healthy use of online space.

A safe and direct help section called ‘Si tienes problemas’[5] (‘If you have problems’) for young people to report and receive immediate help.

[2] Un test para aprender mas. Available at: http://tudecideseninternet.es/aepd/jovenes/de-8-a-14-anos/un-test-para-aprender-mas.html

[3] Selfie Seguro. Available at: https://www.selfieseguro.com/decalogo-10-consejos-selfie-seguro-sin-riesgos/

[4] Pandijuegos. Available at: http://tudecideseninternet.es/concurso-v2/

[5] Si Tienes Problemas. Available at: http://tudecideseninternet.es/aepd/jovenes/si-tienes-problemas.html

In the same way, the Ministry has launched some resources for teachers and families:

- Guides for schools about student data and their protection[6]
- A large selection of resources[7] for teachers and parents, schools and staff working with young people on important issues of internet use.
- Access to online courses created by INTEF (National Institute of Educational Technologies and Teacher Training depending on the Spanish Ministry of Education) on 'Basic protection measures on the Internet'[8]
- Priority channel[9] to communicate the dissemination of sensitive content and request its withdrawal.

Internet Safety Education in the UK

In a report by OFCOM, the media regulator in the UK entitled: ***Children and parents: Media use and attitudes Report 2019*** (OFCOM, 2019) it was reported that during the years of primary school ownership of a device to access the internet increased from 5% for a smartphone and 37% for a tablet to 83% and 59% respectively. Also that by the age of 11, at the end of primary school, 88% of children watch video on-demand or subscription services, 71% have a social media profile and they play over 11.5 hours of games online a week. It is also reported that parents are increasingly concerned about their child seeing self-harm related content, in-game spending and game related bullying. Indeed, fewer parents feel that the benefits of their child being online outweigh the risks compared to five years ago. That said it was also reported that more conversations about online safety are happening in homes and schools than before, with parents twice as likely than a year before to seek support and information online to help keep their children protected.

In a report for OFCOM entitled: ***Revealing Reality, Children's Media Lives- Wave 6, February 2020*** (OFCOM, 2020) reviewed the changing landscape in which children are growing up: new trends, platforms and behaviours. From their sample they found that children in 2019 are increasingly emulating influencers on their social media profiles, that some are provoking attention by posting questions, gamification or sexual content and have seen upsetting content online at some point. A couple of interesting insights from the report include that children are downplaying the amount of sexualised content they see and share online, and are under-reporting how much they use social media and how much they care about their online representation.

This comes as the government reinforce the teaching of online safety within the curriculum which includes in primary schools as part of computing, PSHE (personal, social, health and economic) and SRE (sex and relationships education) teaching. ***Department of Education, Teaching online safety in school, June 2019*** (Dfe, 2019). This aims to equip children with

[6] Guia Para Centros Educativos. Available at: http://tudecideseninternet.es/aepd/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf
[7] Guiales En Internet. Available at: http://tudecideseninternet.es/aepd/guias/guiales-en-internet.html
[8] Presentación Del Sitio Web AseguraTIC. Available at: https://intef.es/Noticias/presentacion-del-sitio-web-aseguratic-seguridad-del-menor-en-medios-digitales/
[9] Canal Prioritario Para Comunicar La Difusión De Contenido Sensible y Solicitar Su Retirada. Available at: https://www.aepd.es/sites/default/files/2019-12/infografia-canal-prioritario.pdf

the knowledge, understanding and skills to use information and communication technology creatively and purposefully. This in large part lies in them becoming digitally literate. As such it is focussed on ensuring children are ‘responsible, competent, confident and creative users of information and communication technology’.

A typical school-wide approach will be to underpin knowledge and behaviour including:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support

Every school works with its students to improve their understanding in all areas of their life both in and out of school, and includes the dissemination of advice to parents. In particular, for Key Stage 2 (ages 7-11) pupils should be taught to:

- Use technology safely, respectfully and responsibly,
- Recognise acceptable/unacceptable behaviour,
- Identify a range of ways to report concerns about content or contact,
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

There are many sources of information to provide information to teachers, parents and children themselves. In addition to those outlined in the last section of this document key ones include:

- Government organisations eg. UK Council for Internet Safety[10]
- E-safety advice and support organisations eg. Childnet[11]
- Parental advice from communications providers eg. Internet Matters[12]
- Support from statutory organisations: eg. police and crime units, such as SEROCU[13]
- National children’s charities and support organisations eg. NSPCC[14]

UK schools work closely with National Online Safety (NOS)[15] who have recently updated their online platform. Parents are encouraged to sign up to the NOS platform. For further support using the NOS platform an email channel is offered.

The following sources of information and support are also recommended:

- Internet Matters[16] specifically designed to support parents.

[10] UK Council for Internet Safety. Available at: https://www.gov.uk/government/organisations/uk-council-for-internet-safety

[11] Childnet. Available at: https://www.childnet.com/

[12] Internet Matters. Available at: https://www.internetmatters.org/

[13] SEROCU. Available at: https://serocu.police.uk/

[14] NSPCC. Available at: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

[15] NOS. Available at: https://nationalonlinesafety.com/

[16] Internet Matters. Available at: https://www.internetmatters.org/

- Parent Info[17] run in conjunction with CEOP, the Child Exploitation and Online Protection command, part of the National Crime Agency.
- Net Aware[18] run by the NSPCC; it has a useful quick search tool, which will give you an overview of the latest apps and trends and give advice on how to minimise their risk.
- UK Safer Internet Centre[19] good advice in general, but particularly useful for tips on how to set up your internet provision at home.

The acknowledgement of the many issues related to online safety and the skills required for children's futures online is generally good in the UK. It is covered in the media, through the online providers of broadband and technology devices, by statutory bodies and is taught in schools. However, it is recognised that many factors still influence the overall understanding throughout the population and the impact of disadvantage. This was recognised by the Government during the COVID crisis in April 2020 when funding was set aside to provide digital devices and internet access to disadvantaged children to access remote learning during lockdown.

However, most importantly for many parents, teachers and children themselves it is the speed at which the digital environment is changing and developing that is one of the most challenging issues. As such focus is often on the education of children to think critically about what they are doing, supporting them to understand the language needed to say no, and how important it is to maintain an open conversation with those that can support them.

Internet Safety Education in Portugal

Digital literacy plays a fundamental role in education and ICT is taught as a subject in its own right in grades 7 to 9. Schools can opt for 90-minute classes for one semester or 45-minute classes over the whole school year. ICT is mainly a practical subject, organised in three areas (the topic of digital safety is covered in all areas):

1. Information;
2. Production;
3. Communication and Collaboration.

Students learn to be active users of computers, networks and the internet. Based on the ICT curricular goals, teachers should create learning situations that promote students' autonomy. Goals should therefore not be seen as a list of topics to be imparted to students in a sequential way, but rather as learning goals, regardless of the sequence that the teacher chooses to follow during each school year. It should therefore be noted that the numbering of the objectives and descriptors does not indicate or suggest a compulsory sequential approach. These learning areas are organised in domains, sub-domains and overall goals.

A new core learning initiative has been taking place from 2017/2018 school year, where 235 school clusters (out of a total of 811) teach ICT from the 5th to the 9th year. ICT as a subject is taught from the 5th year. ICT aims at fostering in students a critical analysis of the function

[17] Parent Info. Available at: https://parentinfo.org/
[18] Net Aware. Available at: https://www.net-aware.org.uk/
[19] UK Safer Internet Centre. Available at: https://www.saferinternet.org.uk/

and power of information and communication technologies and to develop in them the ability to research, process, produce, communicate and collaborate through technologies, in parallel and in an integrated way with research and of information analysis in traditional formats (books, magazines, encyclopedias, newspapers and other information media).

ICT, in the 2nd (grades 5-6) and 3rd (grades 7-9) cycles, goes beyond the development of basic digital literacy, advancing to the domain of the development of students' analytical abilities, through the exploration of computational environments appropriate to their ages.

In the 2nd cycle of elementary education students should know basic concepts that will allow them to progressively (i) adopt a critical, reflected and responsible attitude in the use of digital technologies, environments and services, (ii) develop (iii) develop the ability to communicate appropriately, using digital resources and non-digital resources, and (iv) acquire knowledge of strategies and tools to support creativity through the exploration of ideas and the development of thinking, enabling them to produce creative digital artifacts. These achievements must be progressively extended and deepened through the 5th and the 6th year of schooling.[20]

Internet Safety is regarded as a core subject in Digital Literacy and hence is covered transversely in ICT subjects in school. In addition, Internet Safety issues are included in Media Literacy (in turn included under the broader subject of Citizenship Education). The major Internet Safety topics for 7-12 year olds include:

ICT Literacy

- Understand the need for safe practices in the use of digital devices, with a particular reference to the concepts of private/public;
- Recognise basic security procedures in relation to yourself and others (e.g. data recording of the user);
- Being aware of the impact of ICT on one's daily life;
- Distinguish, in digital context, real situations and/or fiction;
- Understand the need for safe use practices of digital and Internet browsing tools and adopt behavior accordingly;
- Know and use the standards related to copyright and the need to recognise sources;
- Understand the rules for creating and using secure keywords;
- Critically analyse the quality of information.

Media Literacy

- Living in a network/making a network | Risks of being entangled | Cyberbullying
  - Know what one can and should do when one is faced with a situation of cyberbullying

[20] European Schoolnet (2017) Country Report on ICT in Education - Portugal. Available at: http://www.eun.org

  - Recognise the importance of reporting cases of cyberbullying in which they or their friends are involved (as victims or perpetrators)
  - Know that initiatives can and should be promoted to discourage the practice of cyberbullying

- Instrument and culture | Media languages | Access and use practices
  - Learn how to use the Internet safely: develop the ability to distinguish between 'good' and 'bad' information

- Technology | Information and communication technology | Types of screen | Multi-screen
  - Discover and begin to be able to get their bearings in a digital environment
  - Learn to respect the age indications of programs
  - Be sensitive to the risks that can arise on the Internet
  - Identify and understand the opportunities, risks and potential of Internet use
  - Determine the different ways technology impacts on their lives, on that of their friends, family and on society at large
  - Instrument and culture | Media languages | Access and use practices
  - Learn how to use the Internet safely: develop the ability to distinguish between 'good' and 'bad' information

Additionally, Internet Safety is the focus of public and private initiatives, most notably:

- **Internet Segura**[21]

This is a governmental initiative, led by and comprised of key public organisations, that is responsible for the online safety national strategy and for its implementation by establishing links between major actors, making available resources for raising awareness, supporting victims and keeping active vigilance on the internet.

- **SeguraNet**[22]

One of the most important initiatives around Internet Safety is Projeto Seguranet. The SeguraNet Project aims to promote safe use of internet and mobile devices by the school community (students, teachers and parents). The awareness activities for safer Internet use of the SeguraNet Project are as follows:

- to promote the involvement of the existing National Networks - the network of in-service teacher training centres and the ICT Competence Centres – and the experts from the universities in designing awareness tools, training initiatives, and school activities with students participation;
- to support the consortium partners in all national campaigns and actions of the awareness node;

[21] Internet Segura. Available at: https://www.internetsegura.pt/
[22] SeguraNet. Available at: https://www.seguranet.pt/

- to conduct training courses for school teachers and for profession - also from DGE external entities which work with children;
- to promote awareness raising sessions in schools and municipalities (among others) with the support of the national Network of ICT Competency Centers;
- to provide online and offline information and resources in multiple formats for each of the target audiences;
- to promote the SeguraNet Challenges contest that involves students, teachers and parents (covering about 50 000 participants yearly);
- to promote the Digital Leaders Initiative within the school community;
- to promote awareness campaigns (SID and Cybersecurity month) in educational communities;
- to participate in the National Defense Day activities (nationwide initiative involving 130 000 young people yearly);
- to contribute to the Insafe Network and to the working groups of the Safer Internet Consortium;
- to integrate eSafety issues in the National Curricula.

SeguraNet makes available several resources for schools, teachers, parents and pupils, from a MOOC on internet safety for teachers, to games, posters and many others.

- **Miúdos Seguros na Net**[23]

This is a private initiative to support online safety by bringing together families, schools and communities. It sets itself as a discussion forum and displays resources that can be used to implement local initiatives for internet safety.

Internet Safety Education in Lithuania

Legal framework

The internet has long become a natural playground and place of leisure, learning and creativity for young people. Data shows that Lithuanian children are going online at an ever younger age and on a diverse range of devices, often without adult supervision. The exposure to online activity has increased even more during the COVID-19 quarantine as teaching and learning has moved to the virtual environment due to school lockdowns.

As a group, children have specific needs and vulnerabilities in terms of appropriate content, accessibility, safety, development of digital skills and responsible online behavior. Parents,

[23] Miúdos Seguros na Net. Available at: http://miudossegurosna.net/

carers and teachers are faced with constant concerns over how to protect their children against various risks of virtual environment, such as cyber bullying, harmful and illegal content, etc.

Latest research data suggests that kids and teenagers are most often exposed to viruses and unwanted e-mails. According to the police, many of the safety threats come from social networking and other online communication tools[24].

Student's right to learn in a psychologically, emotionally and physically safe environment is stipulated in the Law on Education. The Law on the Protection of Minors against the Detrimental Effect of Public Information (2002) aims to limit minors' access to potentially harmful information). The law:

- defines information that is considered harmful (e.g. display of violence, which is erotic in nature, which encourages self-mutilation of suicide and similar) and limits the dissemination thereof;
- establishes principles of minors' data protection;
- sets out responsibilities of public institutions.

The National Agency for Education, an institution established by the Ministry of Education, Science and Sports, is a member of European Schoolnet[25], a network of EU Ministries of Education. Through the network membership, the Lithuanian agency has better access to first-hand evidence and data in the area of innovation in education on which to base policy recommendations; may provide intellectual support to schools and teachers in their teaching practices; and is able to better promote schools' engagement in innovative teaching and learning approaches.

European Schoolnet is part of a number of internet safety initiatives, for example the *Better Internet for Kids* project. In Lithuania the project is promoted by the Lithuanian Safer Internet Centre (SIC) which was established by the following partners: the Centre of Information Technologies in Education under the Ministry of Education and Science of the Republic of Lithuania, the Communications Regulatory Authority of the Republic of Lithuania, 'Vaikų linija' NGO and the 'Langas į ateitį' Association. The Lithuanian initiative is known under the name 'Saugesnis internetas'/'Draugiškas internetas'[26] (*friendly internet*) and has promoted safer and better use of the internet and mobile technologies among children and young people since 2012. Dozens of other institutions and organisations (including some research centres) are represented on SIC's Advisory Board.

The SIC has developed a national platform that provides three main services for safer internet: an awareness centre, helpline, and hotline services. The teaching of digital literacy and online safety is a shared activity with a variety of ICT-related creative activities

[24] www.delfi.lt (2019) Vaikai ir internetas: ką galime padaryti, kad jie būtų saugūs? Available at: https://www.delfi.lt/partnerio-turinys/sustiprink-imuniteta/vaikai-ir-internetas-ka-galime-padaryti-kad-jie-butu-saugus.d?id=82597185

[25] European Schoolnet (2017) Country Report on ICT in Education - Lithuania. Available at: www.eun.org

[26] "Saugesnis internetas"/"Draugiškas internetas". Available at: www.draugiskasinternetas.lt

supported by actors, including the National Library. From 1 June 2016 to 31 December 2018 7019 reports on illegal or harmful Internet content were received and processed by the hotline[27] and respective action was taken, including reports to police and other responsible state institutions.

The work of the Lithuanian Safer Internet Centre is aligned with national policies, such as the Information Society Development 2014-2020 Programme - 'Digital Agenda of the Republic of Lithuania'[28], contributing to the fulfilment of children's rights and protection from online harm.

Thanks to the programme, a number of awareness raising activities that promote safer internet access to kids have taken place in Lithuania. For example, a number of schools, libraries and other public service organisations across Lithuania organise annual awareness raising activities for the International Safer Internet Day every February. Those range from discussions with students on internet safety-related issues, social networks to production of promotional posters on internet hazards. The schools take the initiative to engage experts, librarians, NGO representatives and activists. Some schools are very active participants of international projects. These include initiatives funded under the Erasmus+ programme, such as eTwinning projects.

One of the latest initiatives that is worth mentioning is CYBERteens[29], a hackathon organised by the Safer Internet Project together with an innovator community called ChangeMakers'ON on 11 February 2020. 19 selected teams from different schools in Lithuania applied their creative design knowledge and developed solutions to tackle 6 different internet safety challenges (e.g. catching and reporting unacceptable content; developing responsible online behavior; raising young people's awareness on online data protection; reducing cyberbullying, etc.). The participants were invited to immerse themselves in creative workshops led by over 30 experts. The most sustainable ideas were given the opportunity to kick-start in real life.

Events like these not only foster awareness but also give first-hand experience to students themselves to develop and implement online safety solutions aimed at their peers or an even wider community of internet users.

In a number of schools, primarily IT teachers take the responsibility of teaching the kids safe online behavior, but sometimes even the subject teachers. For example, at Queen Morta School where every student starting in Grade 3 uses a laptop to learn at school, there is a code of online conduct and the students are regularly asked to prepare presentations on separate

[27] Praneškite apie pastebėtą žalingą turinį internete. Available at: https://pranesk.draugiskasinternetas.lt/

[28] Digital Agenda of the Republic of Lithuania. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a66c0760b04011e3bf53dc70cf7669d9

[29] CYBERteens. Available at: https://www.facebook.com/events/%C5%BEalgirio-arena/saugesnio-interneto-diena-2020-cyberteens-lt-en/2494838937400618/

aspects of online safety, e.g. cyberbullying, online stalking, password protection and others. The parent community got engaged in providing relevant information to the students, teachers as well as other parents through live presentations at school and the school's newsletter.

Schools administrators and teachers have access to a wide range of materials and recommendations available through online sources. As more and more IT is used as part of everyday school curriculum, it is essential that teachers are well equiped to not only use IT effectively, but also to tackle various internet safety challenges that arise. Some non-governmental initiatives concentrate specifically on providing the relevant knowledge to teachers.

For example, in 2018, the Lithuanian Journalism Centre, in partnership with the Embassy of Sweden in Lithuania and the Swedish Institute, produced an online resource for local teachers entitled *The Map of Internet: A Teacher's Toolkit on Internet Media Literacy*[30]. The toolkit provides information and suggested classroom materials and activities on:

- online data collection,
- data sources,
- online privacy,
- social networks, including on fake news, hate speech, bullying and sexting;
- hacking and online crimes;
- and data protection.

The Safer Internet Project offers freely accessible contents for teachers' lessons on various aspects of internet safety[31]: online privacy, online pictures, online fraud, social networking, cyberbullying, inappropriate online content, safer use of smartphones.

The www.epilietis.eu online platform[32] provides information, testing, training and resources on a number of e-services related issues, including online safety. Some schools report having produced their own online safety guidelines, using the resources provided by the platform. Just to give an example, one of the online training sessions offers information to adults who seek to introduce kids to safe online communication and social networking, to teach them how to recognise unsafe online games and respond to questions on social engineering.

The 'Skaitmeninis Moksleivio IQ' (Digital Student IQ)[33]online platform is an outcome of a SAMSUNG-supported digital safety and literacy initiative implemented in a number of Lithuanian schools. The initiative led to the creation of the Digital Etiquette created by Lithuanian students that promotes 10 principles for responsible online behavior. The principles include not believing everything one finds on the internet, being polite and

[30] The Map of Internet: A Teacher's Toolkit on Internet Media Literacy. Available at: https://lzc.lt/leidiniai/interneto-zemelapis-interneto-mediju-rastingumo-metodologine-priemone

[31] The Safer Internet Project. Available at: http://pamoka.draugiskasinternetas.lt/

[32] The www.epilietis.eu online platform. Available at: www.epilietis.eu

[33] The "Skaitmeninis Moksleivio IQ" (Digital Student IQ) online platform. Available at: http://www.skaitmeninisiq.lt/apie-mus%20/

Co-funded by the
Erasmus+ Programme
of the European Union

respectful, reporting bullying, not pretending to be someone else, thinking twice before posting anything, respecting one's privacy, respecting copyright, protecting own data, not getting engaged in pirate activity and not sharing fake news.

As more and more IT is used as part of everyday curriculum at school it is essential that teachers are well equiped to not only use IT effectively, but also to tackle various internet safety challenges that arise. Some non-governmental initiatives concentrate specifically on providing the relevant knowledge to the teachers.

For example, Bit&Byte[34] trained more than a 1000 teachers in 2018-2020 as part of their initiative called 'Technologijų vedliai' (*Leaders in Technology*) supported by Google. The assigned technological mentors trained the teachers to use a number of digital programmes, helped them create assignments and made then more technologically savvy.

Further private initiatives contribute to improved online literacy and awareness. 'Augu internete'[35] (*I grow using the internet*), supported by Telia, have regularly engaged teachers and students (more than 80000 people, according to the initiative's website) through interactive discussions and action. It also provides online content for self study and enables further teaching activities of teachers and parents.

In conclusion, it may be said that despite the fact that the current legal and policy framework is not very explicit, there are a number of public, non-government and private initiatives that contribute to raising kids' awareness of online safety and foster teachers' initiative. A number of schools have created their own guidelines, devote regular attention to training of teachers and teaching students, and engage in discussions and project-based initiatives aimed at better internet for their students.

[34] Bit&Byte. Available at: www.bitbyte.lt
[35] Augu internete. Available at: https://auguinternete.lt/

Co-funded by the
Erasmus+ Programme
of the European Union

DEFINING CYBER EDUCATION AND COMPETENCES

One of the main goals of most ICT education systems is to develop the cyber safety competences. In our analysis of existing literature, we closely aligned the framework to the risks identified in the POST 2019 (Houses of Parliament, 2019) related to online safety education and the requirements of the 21st Centuries Skills document (European Commission, 2007b). As such the POST 2019 delineates between four areas of risk children are susceptible to and proposes the following interventions (Houses of Parliament, 2019):

- Content. This includes age inappropriate material, such as pornography, violent content, and 'fake news'.
- Contact. The risk of a child being radicalised or contacted by people who seek to victimise them.
- Conduct. Risks that involve a child as a perpetrator, or behaviour such as oversharing personal information, cyber-bullying, or creating and sharing sexual images.

Figure 1, 'Cyber Safety and Security Education' (Thiyagu, Santhosh T, 2019) summarises the components of cyber safety education well to include elements of Awareness, Competence, Etiquette, Socialisation, Mindfulness and Cyber Wellness.

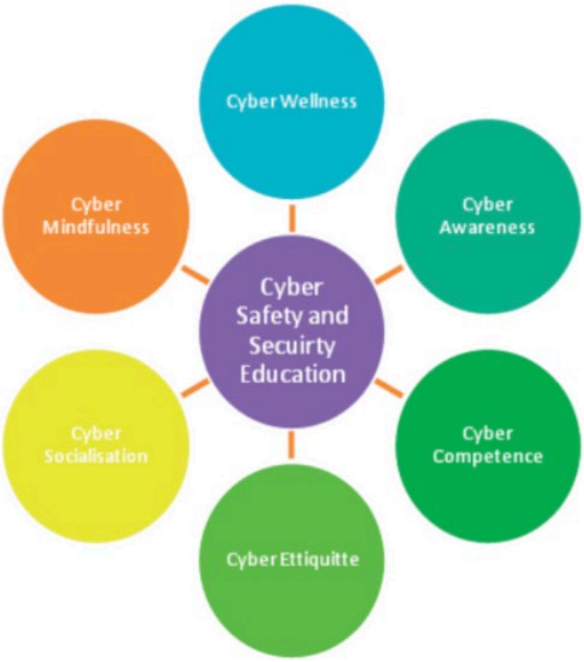


Figure 1. Cyber Safety and Security Education areas

In a more detailed way the 'Education for a Connected World framework' (UK Council for Internet Safety, 2018) focuses specifically on eight different aspects of online safety education:

1. Self-image and Identity

2. Online relationships

3. Online reputation

4. Online bullying

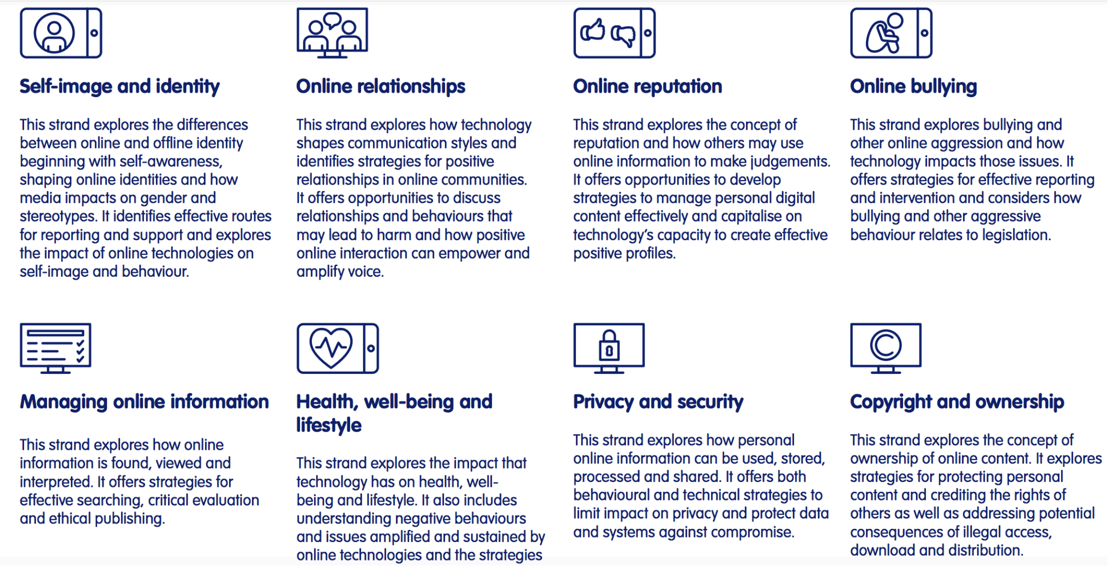
5. Managing online information

6. Health, wellbeing and lifestyle

7. Privacy and security

8. Copyright and ownership

Figure 2, ‘Education for a Connected World Framework’ (UK Council for Internet Safety, 2018) explores the eight areas of competence further in relation to the age group of 7-11 years.



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and how media impacts on gender and stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology’s capacity to create effective positive profiles.

Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation and ethical publishing.

Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies

Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

Figure 2. Education for a Connected World Framework.

Table 1, ‘Cyber Competences’ (Dfe 2019) shows the key cyber competencies and associated skills necessary for school children, as identified by the UK Department of Education.

Table 1: Cyber Competences

Knowledge	Skills examples
Evaluating what you see online	Able to tell if something is a fact, understanding cookies; able to recognise a fake URL

Recognising techniques used for persuasion or manipulation of others	Able to recognise ways in which games and social media companies try to keep users online longer (persuasive/sticky design), and criminal activities such as grooming.
Understanding what acceptable and unacceptable online behaviour looks like	Actively using techniques to defuse or calm arguments (e.g. a disagreement with friends); able to disengage from unwanted contact or content online.
Identifying and dealing with online risks	Able to identify a risk (e.g. sharing information online), understand the consequences and choose the best course of action.
Asking for help when needed	Able to identify trusted adults and find support available within applications etc.

It is essential to recognise the importance of digital skills for children. The individual and household indicator metrics has been developed in 2015 by the EC: DG CONNECT and the Eurostat Information Society Working Group agreed to create and publish a 'Digital Skills Indicator' based on the Digital Competence Framework[36] (developed by JRC and DG EAC, and available for self-assessment on the Europass[37] website). The digital skills indicators include (European Commission, 2016):

1. **Information skills**

   Definition in Digital Competence Framework: identify, locate, retrieve, store, organise and analyse digital information, judging its relevance and purpose.

   - Obtained information from public authorities/services' websites
   - Finding information about goods or services

2. **Communication skills**

   Definition in Digital Competence Framework: communicate in digital environments, share resources through online tools, link with others and collaborate through digital tools, interact with and participate in communities and networks, cross-cultural awareness.

   - Sending/receiving emails
   - Participating in social networks
   - Telephoning/video calls over the internet

[36] Digital competence Framework. Available at: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

[37] Europass. Digital Competences. Available at: https://europass.cedefop.europa.eu/resources/digital-competences

- Uploading self-created content to any website to be shared

3. Problem solving skills

Definition in Digital Competence Framework: identify digital needs and resources, make informed decisions as to which are the most appropriate digital tools according to the purpose or need, solve conceptual problems through digital means, creatively use technologies, solve technical problems, update one's own and others' competences.

A – Problem solving

B – Familiarity with online services

4. Software skills for content manipulation

Definition in Digital Competence Framework: Create and edit new content (from word processing to images and video); integrate and re-elaborate previous knowledge and content; produce creative expressions, media outputs and programming; deal with and apply intellectual property rights and licences.

A – Basic

- Use of word processing software
- Use of spreadsheet software
- Use of software to edit photos, video or audio files

B – Above basic

- Create a presentation or document integrating text, pictures, tables or charts
- Use advanced functions of spreadsheet to organise and analyse data (sorting, filtering, using formulas, creating charts)

Co-funded by the
Erasmus+ Programme
of the European Union

THE CYBERADVENTURE EDUCATION FRAMEWORK

Considering the examination of the current state, as described in the previous sections, and following the current conventions of defining ICT competencies, in this project the trend of separation of competences into three constituent-categories is followed: knowledge, skills and attitudes. The latest reports issued by Eurydice[38] the 'Education for a Connected World Framework' (The UK Council for Internet Safety, 2018) and other works reviewed in this document converge to provide a complete overview of what cyber education should include for the ages of the designated target-group (6 -10 year olds).

Thus, the designed activities should be of an original, realistic and experiential nature. Table 2 presents the key competences that should be treated in primary education.

Table 2: CyberAdventure Competences Framework

Knowledge	Skills	Attitudes
Self-image and identity – exploring the differences between online and offline identity.	• Self-awareness • Shaping online identities and how media impacts on gender and stereotypes • Effective routes for reporting and support • Impact of online technologies on self-image and behaviour • Ability to explain what is meant by the term 'identity'.	Experience of having and managing a digital reputation
Online relationships - exploring how technology shapes communication styles and identifies strategies for positive relationships in online communities. Opportunities to discuss relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.	• Ability to describe ways people who have similar likes and interests can get together online. • Using technology-specific forms of communication (e.g. **emojis**, **acronyms**, **text speak**). • Understanding of risks of communicating online with strangers.	View of how relationships are formed, maintained and ended differently online

[38] Eurydice. Available at: https://eacea.ec.europa.eu/national-policies/eurydice/

	• Ability to explain why one should be careful who one can trust online and what information can be trusted them with. • Understanding how one’s and other people’s feelings can be hurt by what is said or written online. • Knowledge of strategies for safe and fun experiences in a range of online social environments. • Understanding of how to be respectful to others online. • Knowledge of the ways of reporting problems online.	
Online reputation - exploring the concept of reputation and how others may use online information to make judgements. Opportunities to develop strategies to manage personal digital content effectively and capitalise on technology’s capacity to create effective positive profiles.	• Knowledge of the ways that some of the information about oneself online could have been created, copied or shared by others. • Ability to search for information about oneself or other individual online and create a summary report of the information found. • Ability to describe ways that information about people online can be used by others to make judgements about an individual.	Young people will become critical readers of online information

Online bullying - exploring bullying and other online aggression and how technology impacts those issues. Strategies for effective reporting and intervention. Consideration on how bullying and other aggressive behaviour relates to legislation.	• Understanding of what bullying is. • Rules about how to behave online and how to follow them. • Ability to identify some online technologies where bullying might take place. • Ability to describe ways people can be bullied through a range of media (e.g. image, video, text, **chat**). • Understanding of the need to think carefully about how one's content might affect others, their feelings and how it may affect how others feel about them. • Ability to recognise when someone is upset, hurt or angry online. • Knowledge of how to block abusive users. • Ability to report online bullying on the familiar apps. • Knowledge of the helpline services and what to say and do if their help was needed (e.g. **Childline**). • Ability to capture bullying content as evidence (e.g **screen-grab**, **URL**, **profile**). • Ability to identify ways to report concerns both in school and at home about online bullying.	The impact of being online for young people's mental health

Managing online information - exploring how online information is found, viewed and interpreted.	• Being able to use key phrases in search engines. • Being able to explain what **autocomplete** is and how to choose the best suggestion. • Being able to search for information within a wide group of technologies (e.g. social media, image sites, video sites). • Understanding of some of the methods used to encourage people to buy things online (e.g. advertising offers; **in-app purchases**, pop-ups) and can recognise some of these when they appear online. • Understanding that some people one 'meets online' (e.g. through social media) may be computer programmes pretending to be real people. • Understanding of why lots of people sharing the same opinions or beliefs online does not make those opinions or beliefs true. • Being able to use different search technologies. • Being able to evaluate digital content and to explain how to make choices from search results.	Experiencing strategies for effective searching, critical evaluation and ethical publishing.

	• Being able to explain key concepts including: data, information, fact, opinion belief, true, false, valid, reliable and evidence, and to differentiate between them. Understanding of what criteria have to be met before something is a ‘fact’. • Understanding of the difference between online **mis-information** (inaccurate information distributed by accident) and **dis-information** (inaccurate information deliberately distributed and intended to mislead). • Being able to explain what is meant by ‘being sceptical’. Being able to give examples of when and why it is important to be ‘sceptical’. • Being able to explain what is meant by a ‘**hoax**’and why one needs to think carefully before forwarding anything online. Being able to explain why some information found online may not be honest, accurate or legal, even if it is found on a large number of sites. Being able to assess how this might happen (e.g. the sharing of misinformation either by accident or on purpose). • Understanding of how search engines work	

	and how results are selected and ranked. • Able to demonstrate the strategies required for evaluating digital content. • Being able to explain how and why some people may present ‘opinions’ as ‘facts’. • Being able to define the terms ‘influence’, ‘manipulation’ and ‘persuasion’ and explain how one might encounter these online (e.g. advertising and ‘ad targeting’). • Being able to demonstrate strategies to enable me to analyse and evaluate the validity of ‘facts’ and to explain why using these strategies is important. • Being able to identify, flag and report inappropriate content.	

Health, well-being and lifestyle - explores the impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.	• Understanding of why spending too much time using technology can sometimes have a negative impact on an individual. • Being able to identify times or situations when there might be a need for limiting the amount of technology use. • Being able to describe ways technology can affect healthy sleep. • Being able to describe some strategies, tips or advice to promote healthy sleep with regards to technology. • Being able to describe common systems that regulate age-related content (e.g. **PEGI**, **BBFC**, parental warnings) and describe their purpose. • Being able to assess and action different strategies to limit the impact of technology on my health (e.g. night-shift mode, regular breaks, posture, sleep and exercise). • Understanding of the importance of self-regulating one’s use of technology; being able to demonstrate the strategies to do this (e.g. monitoring one’s time online, avoiding accidents).	Problem-solving Understanding work-life balance and healthy choices

Privacy and security - exploring how personal online information can be used, stored, processed and shared.	• Being able to give reasons why I should only share information with people one chooses to and can trust. Understanding of asking a trusted adult if one is not sure or feels pressured. • Understanding of reasons why passwords are important. • Being able to describe simple strategies for creating and keeping passwords private. • Understanding of how connected devices can collect and share one's information with others. • Being able to describe strategies for keeping one's personal information private, depending on context. • Being able to explain that others online can pretend to be other people, including one's friends and to suggest reasons why they might do this. • Being able to explain how internet use can be monitored. • Being able to create and use strong and secure passwords. • Understanding of how many free apps or services may read and share private information (e.g. friends, contacts, likes,	Ability to exercise behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

	images, videos, voice, messages, **geolocation**) with others. • Understanding of how and why some apps may request or take payment for additional content (e.g. in-app purchases) and explain why one should seek permission from a trusted adult before purchasing. • Use of different passwords for a range of online services. • Being able to describe effective strategies for managing those passwords (e.g. **password managers**, acronyms, stories). • Knowledge of what to do if one's password is lost or stolen. • Being able to explain what app permissions are and to give some examples from the familiar technology or services. • Being able to describe simple ways to increase privacy on apps and services that provide privacy settings. • Being able to describe ways in which some online content targets people to gain money or information illegally; being able to describe strategies to help me identify such content (e.g. **scams**, **phishing**).	

Copyright and ownership - exploring the concept of ownership of online content. Strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.	• Being able to explain why and how copying someone else's work from the internet without permission can cause problems. • Being able to assess and justify when it is acceptable to use the work of others. • Being able to give examples of content that is permitted to be reused. • Being able to demonstrate the use of search tools to find and access online content which can be reused by others. • Being able to demonstrate how to make references to and acknowledge sources used from the internet.	Ethical decision making.

BENCHMARKING

CyberAdventure project will design a measurement tool to assess the effect of participation in the CyberAdventure Game on young children's skills, attitudes towards using the internet safely (Appendix A: Cyber Skills Benchmarking Tool).

CONCLUSION

Research shows that children go online at an ever-younger age and the time spent online is steadily increasing (European Commission, 2007a). While the internet offers many opportunities for learning, communication, creativity and entertainment, it also opens up certain risks to vulnerable users, such as children (European Commission, 2019). The Online Safety Education remains a priority for the EC. The EC established the Safer Internet Programme, followed by other programmes, namely the current European Strategy for a Better Internet for Children COM(2012) (European Commission, 2012).

The review of internet safety education conducted by the partners shows that the challenges facing parents and educators in teaching children about internet safety remain very significant. Internet safety education is slowly getting embedded in school curricula and there are some good existing teaching and learning resources available to help with this process. The CyberAdventure game will be developed to further assist children, parents and educators in learning and teaching about internet safety. The *Framework for the Key Cybersafety Competences* will provide a solid foundation on which the game will based, providing a valuable contribution to the four participating countries (the UK, Portugal, Lithuania and Spain), as we as the wider education and learning communities.

REFERENCES

Department of Education (Dfe 2019) *Teaching online safety in school. Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects*. Available at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools [Accessed 28 April 2020]

EEAS (2019) *Keeping children safe in the digital world*. Available at: https://eeas.europa.eu/delegations/un-geneva_en/57673 [Accessed 19 May 2020]

European Commission (2007a) *European Framework for Safer Mobile Use by Younger Teenagers and Children*. Available at: https://ec.europa.eu/digital-single-market/en/european-framework-safer-mobile-use-younger-teenagers-and-children [Accessed 13 May 2020]

European Commission (2007b) *e-Skills for the 21st century: fostering competitiveness, growth and jobs COM(2007).* Available at: https://ec.europa.eu/growth/content/e-skills-21st-century-fostering-competitiveness-growth-and-jobs-1_en [Accessed 19 May 2020]

European Commission (2009) *The Safer Social Networking Principles for the EU*. Available at: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf. [Accessed 13 May 2020]

European Commission et al (2011) *Protecting Children in the Digital World COM(2011)*. Available at: https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2011/0556/COM_COM(2011)0556_EN.pdf [Accessed 19 May 2020]

European Commission (2012) *European Strategy for a Better Internet for Children COM(2012) 196 final*. Available at: https://ec.europa.eu/digital-single-market/en/news/european-strategy-better-internet-children-com2012-196-final. [Accessed 13 May 2020]

European Commission (2016) *A new comprehensive Digital Skills Indicator*. European Commission (25/02/2016). Available at: https://ec.europa.eu/digital-single-market/en/news/new-comprehensive-digital-skills-indicator [Accessed 25 January 2020]

European Commission (2018a) *EU Child Safety Online Project*. Available at: http://www.euchildsafetyonlineproject.com/ [Accessed 19 May 2020]

European Commission (2018b) *Alliance to better protect minors online*. Available at: https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online [Accessed 19 May 2020]

European Commission (2018c) *Self-regulation for a Better Internet for Kids*. Available at: https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids [Accessed 19 May 2020]

European Commission (2019) *A European Strategy to deliver a Better Internet for our Children*. Available at: https://ec.europa.eu/digital-single-market/en/european-strategy-better-internet-children [Accessed 13 May 2020]

European Parliament (2015) *Promoting youth entrepreneurship through education and training*. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2015-0292_EN.html [Accessed 19 May 2020]

European Parliament (2018). *Eurobarometer*. Available at: https://europarl.europa.eu/at-your-service/en/be-heard/eurobarometer [Accessed 13 May 2020]

FRA (2018) *The European Union Agency for Fundamental Rights*. Available at: https://fra.europa.eu/en [Accessed 19 May 2020]

Houses of Parliament (2019) *UK Parliament Online Safety Education POST-PN-0608*. Available at: https://post.parliament.uk/research-briefings/post-pn-0608/ [Accessed 19 May 2020]

Ley Orgánica 3/2018. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* Available at: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf [Accessed 19 May 2020]

Ley Orgánica 3/2019. *Ley Orgánica 3/2019, de 12 de marzo, de reforma del Estatuto de Autonomía de la Comunitat Valenciana en materia de participación de la Generalitat Valenciana en las decisiones sobre inversión del Estado en la Comunidad Valenciana*. Available at: https://www.boe.es/eli/es/lo/2019/03/12/3 [Accessed 19 May 2020]

OFCOM (2019) *Children and Parents: Media Use and Attitudes Report*. Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2019 [Accessed 19 May 2020]

OFCOM (2020) *Revealing Reality, Children's Media Lives- Wave 6.* Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/190524/cml-year-6-findings.pdf [Accessed 19 May 2020]

The Royal Society (2017) *After the Reboot: The State of Computing Education in UK Schools and Colleges*. Final report. Available at: https://royalsociety.org/-/media/policy/projects/computing-education/pye-tait-teacher-survey-report.pdf [Accessed 19 May 2020]

Thiyagu, Santhosh T (2019) Cyber safety and security education. Lulu Publication. Available at:

https://books.google.co.uk/books?id=YYvHDwAAQBAJ&printsec=frontcover [Accessed 19 May 2020]

UK Council for Internet Safety (2018) *Education for a Connected World framework*. Available at: https://www.gov.uk/government/publications/education-for-a-connected-world [Accessed 28 April 2020]

APPENDIX A: Cyber Skills Benchmarking Tool

	Knowledge area	Key indicators
1	**Self-image and identity**	• I can describe ways in which media can shape ideas about gender. • I can identify messages about gender roles and make judgements based on them. • I can challenge and explain why it is important to reject inappropriate messages about gender online. • I can describe issues online that might make me or others feel sad, worried, uncomfortable or frightened. • I know and can give examples of how I might get help, both on and offline. • I can explain why I should keep asking until I get the help I need.
2	**Online relationships**	• I can show I understand my responsibilities for the well-being of others in my online social group. • I can explain how impulsive and rash communications online may cause problems (e.g. flaming, content produced in live streaming). • I can demonstrate how I would support others (including those who are having difficulties) online. • I can demonstrate ways of reporting problems online for both myself and my friends.
3	**Online reputation**	• I can explain how I am developing an online reputation which will allow other people to form an opinion of me. • I can describe some simple ways that help build a positive online reputation.
4	**Online bullying**	• I can describe how to capture bullying content as evidence (e.g **screen-grab**, **URL**, **profile**) to share with others who can help me. • I can identify a range of ways to report concerns both in school and at home about online bullying.

5	**Managing online information**	• I can use search technologies effectively. • I can explain how search engines work and how results are selected and ranked. • I can demonstrate the strategies I would apply to be discerning in evaluating digital content. • I can describe how some online information can be opinion and can offer examples. • I can explain how and why some people may present 'opinions' as 'facts'. • I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how I might encounter these online (e.g. advertising and 'ad targeting'). • I can demonstrate strategies to enable me to analyse and evaluate the validity of 'facts' and I can explain why using these strategies are important. • I can identify, flag and report inappropriate content.
6	**Health, well-being and lifestyle** - explores the impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.	• I can describe common systems that regulate age-related content (e.g. **PEGI**, **BBFC**, parental warnings) and describe their purpose. • I can assess and action different strategies to limit the impact of technology on my health (e.g. **night-shift mode**, regular breaks, correct posture, sleep, diet and exercise). • I can explain the importance of self-regulating my use of technology; I can demonstrate the strategies I use to do this (e.g. monitoring my time online, avoiding accidents).
7	**Privacy and security -** exploring how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.	• I use different passwords for a range of online services. • I can describe effective strategies for managing those passwords (e.g. **password managers**, acronyms, stories). • I know what to do if my password is lost or stolen. • I can explain what app permissions are and can give some examples from the technology or services I use. • I can describe simple ways to increase privacy on apps and services that provide privacy settings. • I can describe ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content (e.g. **scams**, **phishing**).

8	**Copyright and ownership -** exploring the concept of ownership of online content. Strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.	• I can demonstrate the use of search tools to find and access online content which can be reused by others. • I can demonstrate how to make references to and acknowledge sources I have used from the internet.