STRANDS

Transforming schools in the digital era

Schools in Transformation with Readiness, Adaptations and Nurturing Digital Skills

E- SAFETY MANUAL FOR FAMILIES AND STUDENTS

Grant agreement	2021-1-IT02-KA220-SCH-000032589
Programme	Erasmus +
Key action	Cooperation for innovation and the exchange of good practices
Action	Strategic Partnerships: Cooperation partnerships in school education
Project acronym	STRANDS
Project title	Schools in Transformation with Readiness, Adaptations and Nurturing Digital Skills
Project starting date	01/12/2021
Project duration	24 months
Project end date	01/12/2023
Project Activity (A)	PR4
Deliverable title	E-safety Manual for Families and Students
Produced by	P3 – Redial Partnership

Consortium:

Promimpresa

Emphasys CENTRE

icep

EDUPUNTOZERO

RE DIAL
Research | Enterprise | Development | Inclusion | Arts | Learning

Contents

Introduction

The STRANDS project "Schools in Transformation with Readiness, Adaptations and Nurturing Digital Skills', co-funded by the Erasmus+ Programme (Project Number: 2021-1-IT02-KA220-SCH-000032589) aims to ease the transition of educators and learners into blended learning and distance learning by supporting them in embracing digital methodologies into learning practices, while building emotional bonds.

This manual entitled "E-Safety Manual for Families and Students" has been produced in the framework of the STRANDS project by all the members of the consortium composed of 5 partners from 4 European countries: Promimpresa from Italy, ICEP from Slovakia, Emphasys from Cyprus, Edupuntozero from Italy and Redial from Ireland. The preparation, development and implementation of this manual have been carefully coordinated by Redial, Ireland.

This manual represents the fourth result of the project whose goal is to address young people's needs to use digital technologies and engage effectively and safely in online activities. In order to do so, the E-Safety Manual gathers resources that offer practical tips and advice on different aspects of keeping young people safe online and protecting them from risks such as cyberbullying, dangerous online challenges, internet addiction, loss of privacy and scandals related to the misuse of personal data, web-tracking, spreading of fake news, image-based abuse and sexting. It also contains a map of local and international services providing support and case studies in order to guide and support parents, guardians, and carers, to set boundaries around online behaviour and technology use as they play a key role in preparing young people to be digitally mature.

Indeed, some of the risks posed to students have long alerted policy makers to the need to make safety an essential part of digital education. Young people are increasingly exposed to an open and collaborative online culture, which allows them to access educational resources, and maintain friendships and relationships with family and friends, and to create and share content (Collin, Rahilly, Richardson, & Third, 2011). However, youth is considered a vulnerable category, because of their developmental stage, where they need to push boundaries and take risks in order to find their identities and become independent young adults. Their risk-taking behaviours can lead to negative outcomes (Viner, 2005), hence, parents are required to remain actively involved regarding the nature of their children's online activities, and to continue to communicate about their use of technology.

STRANDS project aims to contribute to these efforts by raising awareness of online safety and potential online dangers among families and students. It wants to increase the involvement of parents in students' education and improve communication and

synergies between schools and families at risk of online danger. This manual is replicable and transferable to other contexts as it is a useful resource for all citizens, and in different contexts, such as in youth work and in community sectors. It is also translated in all partner languages to benefit all European citizens and institutions.

Benefits of online opportunities and importance of synergy between schools and families

The European Commission has been actively involved in the digital transition and the digitalisation has advanced ever since the sanitary crisis impacted the lives of many thousands of students, schools and families across the continent. According to Eurostat, the proportion of young people in the EU who took an online course climbed by 2.6 times from 13 % to 34 % between 2019 and 2021. As a result, in 2021, 71% of young Europeans reported having at least basic digital skills. The benefits of online teaching and learning are numerous and the use of digital technologies can ease the personal and professional

lives of a lot of people unless they are used in a bad or improper way. Therefore, there is a need to encourage the development of trustworthy technologies and open up new online opportunities for young people in a wide range of sectors in order to foster an open and democratic society.

Young people in Europe have access to a variety of opportunities thanks to the internet and other online technologies that lead to advantages such as participation and civic engagement; creativity and self-expression; identification and social connection; education, learning, and digital literacy. Information and communication technologies (ICTs) have become an integral part of people's daily lives. Many young people in the EU now use the internet to perform a variety of activities in the framework of their work, education, entertainment, administration, networks and other areas of interest.

In sociology the concepts of structure and agency are used to explain what influences human behaviour. In this specific context, these concepts can help define what youth online opportunities and advantages are. Structure is defined as the rules and resources that can enable or limit young people such as parental supervision, guidelines and limitations, physical resources for using the internet at home and at school etc. When it comes to the term agency, here it doesn't refer to people's intentions but rather to their actual actions related to their free will, their motivation, creativity, their own choices and initiatives. As a result, online opportunities depend not only on young people's actions but also on their literacy skills as well as their communicative abilities and digital competencies. Indeed all these competencies and soft skills combined are necessary not only for social connection and identity but also for online content creation which implies researching, using, transforming and expanding information. As can be seen, some of the skills mentioned can be acquired at home and some at school. Thus, the child has two primary learning environments: parents and a school or other institution. That is why the synergy between families and schools is important.

A wider framework of familial, social, cultural, political, and economic factors affects how young people engage in digital activities. Most specifically, **parental involvement increases a child's learning achievement and performance.** Indeed, improved levels of literacy, good behavioural and attitude improvements, increased confidence and self-esteem, and many other benefits can be seen when families are involved in their children's education. Moreover, it enables parents to have a greater understanding of their child's development and of the solutions that can be taken to meet their needs.

However, there is frequently a gap between the two learning environments. The two biggest obstacles to effective parental involvement at the school level are time and accessibility. As a result, the child doesn't benefit from all the advantages that come from

a positive relationship between home and school. To close this gap and fully reach the benefits of the synergies between schools and families, it may be possible to use the internet which represents the third centre of learning. Indeed, more and more classrooms are using digital teaching/learning methods which enable both parents and students to easily have access to the resources and the content at home as well. As a result, it is simple for the parent to monitor what is going on in the classroom and to support their children. As a matter of example, ICTs can also help parents and teachers identify a child's areas of strength and weakness and follow his or her learning levels by feeding the results of an assessment into a digital system that will be able to design unique and adapted learning paths for each student. In a nutshell, technology can facilitate synergies between homes and schools by making information and resources available for all entities involved in the education process but also by providing parental assistance and academic support in cases where parents lack the necessary knowledge to help their children with particular subjects or other issues related to behaviour.

To reinforce the synergies between schools and families, parents need to be involved not only in their children's education but also directly with the school. Most specifically, they need to cooperate together and support each other in order to create a safer learning environment for young people. Epstein's work refers to "school, family and community partnership" instead of parental "involvement" to highlight the role of parents and recognise the importance of shared responsibility at home and at school. In this way, this "partnership" can create two way communication channels between school and home in order to communicate effectively with families about the benefits and opportunities of online education but also to help monitor the use of technologies at home. To achieve these goals families must be involved in the academic learning and activities of their children at home but also in school through committees or parent organisations in order to be more aware of this topic. Besides, support, services and additional resources for families and students can be acquired by community groups such as organisations or associations working in this field.

Therefore, this "partnership" is important specifically in our context as it enables both parties to establish a responsive dialogue, set up shared goals and take joint action to prevent risks encountered online by youth. As a matter of fact, young people can be exposed to several kinds of dangers online due to misuse of the internet, ignorance about threats, external abuse etc. That is why the following section aims to identify the risk and consequences of these different dangers and give tips for young people and families on how to stay safe online.

Resources on how to prevent risks of digital presence of youth

Maximising children's privacy in the digital era means acting in their best interest, which sometimes is not an easy thing to do. Here are **transversal tips to prevent the risk for families**, while below you can find tips to prevent the risk for families for each topic:

- **Physical activities:** Ensuring that family members have physical (sport and outdoors) activities programmed that do not include focused use of digital and online tools.
- **Discussion:** Family members should find time to interact and discuss what they may encounter. The point of those interactions is to semi-directly influence the way that young people interpret information that they come across online. Educate family members about privacy, explain the risks associated with sharing personal information online and the need to be cautious about who they share information with, help them understand the importance of personal data and privacy, teach your child about the risks of web tracking and how to protect their online privacy, explain how cookies and other tracking technologies work, and encourage them to be cautious about the information they share online.
- **Privacy settings:** Encourage your family members to use strong privacy settings on social media and other online accounts. This can help limit the amount of personal information that is shared with others. Encourage your child to use privacy-focused web browsers that block third-party trackers and prevent websites from collecting their data. Examples of such browsers include Brave, Mozilla Firefox with enhanced tracking protection, and Tor.
- **Strong password:** Encourage your family members to use strong, unique passwords for each online account. This can help prevent unauthorised access to their accounts. Learn how to use a password manager (a password manager is an app on your smartphone, tablet or computer that stores your passwords, so you don't need to remember them).

Here are **transversal tips to prevent the risk for young people**, while below you can find tips to prevent the risk for young people for each topic:

- **Consider before sharing:** Consider your actions carefully before sharing anything on digital media because it might remain online forever and be used against you in the future. Don't divulge personal information like your address, phone number, or school name.
- **Learn how to manage privacy settings:** Read and learn how to manage the privacy options for your preferred social media apps. You can choose who may view your profile, send you direct messages, and leave comments on your posts. Educate yourself about web tracking and online privacy. Understand how cookies and other tracking technologies work, and be aware of the risks they pose. By being informed, you can make better decisions about protecting your personal information. Utilise privacy-focused web browsers that block third-party trackers and prioritise your online privacy. Browsers like Brave, Mozilla Firefox with enhanced tracking protection, and Tor can help safeguard your data while you browse the internet.
- **Report offensive content:** Immediately report offensive remarks, messages, images, videos and profiles. If you see something online that makes you uncomfortable or if you think someone is trying to scam you, report it to the appropriate authorities/social media.
- **Use strong passwords:** Use strong and unique passwords for your online accounts. Avoid using the same password for multiple accounts, as this can increase the risk of unauthorised access to your personal information. Avoid sharing passwords with anyone.

Risks to be monitored:

1. Personal well-being

Partner	P1
Author	PROMIMPRESA SOCIETA' BENEFIT SRL
Topic to be addressed and its definition	**Personal well-being** is about the impact that the use of digital technology has on the physical and mental health of an individual.
Risk and consequences	Health risks and consequences, just like their counterpart solutions, can be linked to two primary categories, which are the quality and quantity of interaction and apply for both the physical and mental aspects of the individual's health. Spending excessive amounts of time in front of a device can have the following impact on a person's physical health: - Vision (impaired or distorted eyesight) - Postural deformation - Musculo-skeletal imbalances - Breathing (which can have a further effect on one's emotional states, ability to focus and remember) With regards to mental and emotional well-being, the consumption of too much information or unhealthy content can also have negative effects, such as: - Feeling stressed - Experiencing anxiety - Feelings of depression - Experiencing frustration and/or Inferiority - Inability to focus The occurrence of each problem depends on and is dictated by the student's personal habits, personality and social environments which include both in and out of school circles, activities, and family.

Signs to be monitored	With regards to **the quantity of time spent** on digital devices or engaged in activities related to the use of online tools, the following suggestions can be made for monitoring: - The total amount of time spent on digital activities and devices - The amount of time spent without taking a break - The number of times the individual reaches for their device out of habit With regards to **the quality of interaction** and time spent, things to be monitored are: - Overall mood - Ability to concentrate for extended periods of time without interruption (90 to 120 minutes) - Type of content consumed - Which hours of the day is one engaging with their digital devices and in digital activities
Tips to prevent the risk for families	Preventing unhealthy digital habits and their consequences starts with the things already mentioned. Paying attention to the occurrence of any of the mentioned risky behaviours and their consequences, as well as monitoring the described metrics. This is important, as it is going to provide you with the necessary data to understand what problems you are dealing with and what would constitute an adequate solution. Some of the strategies described in the *web-tracking* section can help you gather the data you need about the behavioural tendencies of students. Once you have that, you can tailor your solution according to your needs.

	Ensuring that family members have physical (sport and outdoors) activities programmed that do not include focused use of digital and online tools is a great way to start. Making sure that physical activity is also incorporated between sessions is the next step. This means that every 90 to 120 minutes of digital engagement, the students are to take a 20-minute break, which includes one of the following activities: - Moving, walking - Stretching - Other physical exercise - Looking into the distance to relax the eyesight and regain visual ability This means that one should avoid immediately taking on another activity like reading or writing, which engages the body and brain in a position that is similar to the ones that digital consumption presupposes. Regarding the quality of content consumed – family members should find time to interact and discuss what they may encounter. The point of those interactions is to semi-directly influence the way that students interpret information that they come across online. It also builds trust among family members, encouraging children to share. This means that adults are required to approach the topics of interest and type of content their children prefer to consume with an open mind and curiosity first; judgement needs to be abstained, in order to enter the young person's world. Naturally, this doesn't mean that the content that they engage with is not to be controlled and interfered with, if deemed unnecessarily explicit and harmful (mentally or emotionally). This is why, critique of types of content and information should come from a place of understanding, and exchanged through proper dialogue and interaction between both parties. The better communication and rapport are established between parental figures and their children, the more insight the former will have about the mental and emotional well-being of their

	adolescents, and the more influence they will have, enacting corrective behaviour.
Tips to prevent the risk for young people	1. **Making the time spent online purposeful and productive** Oftentimes we find ourselves doom scrolling content, instead of consuming any of it with intent. We often open countless tabs, save videos and posts as "favourites", only to leave them in the "see later" section of our profile - never to be revisited again. Spending time purposefully means that we can actually plan the amount of time that we are going to spend on social media, as well as the content we plan on exploring - this may be a course, a TedTalk, or simply catching up with people or others in our DMs (Direct Messages). The main point is that we know why we are online, what we want to do, and that we have a certain amount of time dedicated to that activity for us to enjoy, and not be hard on ourselves for doing it. 2. **Dealing with the habit of checking** More often than not, we don't even want to be on social media, we "simply find ourselves there" out of habit. We are used to checking our devices and keeping our brains occupied. When you are looking to focus on something and recognise that your device is not helping, the easiest thing to do is: - Switch off your sounds - Turn off the notifications - Place it on the screen down - Keep it out of reach (best left in the other room) However, there is the situation where you may actually need your device for a task. In this case, you will need a more elegant solution, like an app that blocks your visits to any website that you'd like to keep out of reach for the time being.

For Windows users, one such app is "Cold Turkey".

The equivalent for iOS is "Freedom".

Using both is easy and it literally blocks the distractions - even if you open up a tab to check your preferred newsfeed out of habit, the only thing you'll see is a blank screen with a message that reminds you of the good you did for yourself.

3. Taking physical and mental breaks

One thing that we rarely realise is what a healthy break looks like. It often happens that the moment we are done with a demanding task, we flip out our device out of habit and look for something to enjoy, albeit not productively (we've already discussed that). However, even if we don't recognise it at first, we haven't really done much to take an actual break from being *engaged*.

Try for a moment, to see yourself from a third person perspective while engaged in a task and compare that to being on social media or watching a movie; not a lot is changing. We are retaining a similar body posture, looking at the same (or similar) screen, from the same distance.

This is to say that, even though we think we are taking a break from action - there's nothing in our brain, body and behaviour to tell us that we are actually doing so.

And this is why it is important to take an actual break every 90-120 minutes, which includes a change of:

- Place
- Body position
- Mental engagement

Exercice is also a great way to switch things around. This doesn't necessarily mean going to the gym; doing a few squats and stretches could also do the trick as it also helps with setting off some of the negative effects from sitting too much and hunched over.

You can also consider a shower, a brief meditation practice, going out for a few steps or simply looking outside into the distance, which is a well-observed technique to relax the eyes and allow them to

	regain their ability.
Technical tools	- https://getcoldturkey.com/ - https://freedom.to/freedom-for-ios - https://apple.co/40DwWkk (Focus List App) - https://apple.co/3ol9Hs7 (MinimaList App)
Existing national and EU campaigns	- https://repubblicadigitale.innovazione.gov.it/it/i-progetti/ - https://www.benesseredigitalescuole.it// - https://educazione.comune.fi.it/dalle-redazioni/benessere-digitale - https://www.adolescienza.it/eventi/digitalmente-al-via-la-seconda-edizione-per-promuovere-il-benessere-digitale-nelle-scuole/
Positive narrative	While there are multiple risks to personal well-being that require proper awareness among young users, it is also true that technology offers opportunities to enhance one's well-being. Listed below are some examples: - **Social connection:** Digital technology can help individuals stay connected with friends and family, even if they are geographically distant. Social media platforms, video conferencing, and messaging apps can provide opportunities for social interaction, which can help combat feelings of loneliness and social isolation. - **Personal safety:** Digital technology can provide safety features such as location tracking and parental controls, which can help parents and caregivers monitor and protect their children's online activity and keep them safe from online risks. - **Creative expression:** Digital technology can provide opportunities for children and teens to express their creativity through platforms such as music production software, graphic design tools, and video editing software, which can help improve their self-esteem and sense of accomplishment. - **Educational resources:** Digital technology can provide access to a wide range of educational resources such as

	online courses, videos, and interactive games, which can help children and teens learn new skills and concepts, and improve their academic performance. - **Physical activity:** Digital technology can provide opportunities for children and teens to engage in physical activity, such as using fitness trackers or dance games, which can improve their physical health and well-being. - **Special needs support:** Digital technology can provide specialised tools and resources for children and teens with special needs, such as speech therapy apps, assistive technology, and online support groups, which can help them overcome challenges and improve their quality of life. Overall, the use of digital technology has the potential to positively impact both physical and mental health in a variety of ways. However, as mentioned earlier, it is important to use digital technology in a balanced and responsible way to maximise its benefits while minimising its potential risks.
Case study	The case study presented here was conducted by several doctors from the Department of Pediatrics at Chieti Hospital, analysing the "Text Neck Syndrome in Children and Adolescents". A 16-year-old girl was admitted to the paediatric unit with a medical referral indicating she was experiencing headaches, dizziness, and acute neck pain. She presented symptoms of headache, subjective vertigo, and ataxia. There was no reported fever or history of trauma. Medical tests were normal, but an MRI showed an inversion of the normal cervical lordosis and posterior disc protrusion at the C4-C5 level, leading to a diagnosis of text-neck syndrome. The patient was advised by the orthopaedic consultant and physiatrist to maintain ergonomic postures during study hours, limit the use of mobile devices, and not exceed 2 hours per day of touch-screen device usage. Insufficient physical activity and excessive sedentary time, especially in front of screens, have been linked to negative effects on children's psychophysical well-being. The prevalence of musculoskeletal neck

	pain is increasing among children and adolescents, with one notable factor being the widespread use of digital technology devices. Failure to maintain proper posture while using these devices gradually increases stress on the cervical spine, contributing to the development of neck pain.

2. Cyber-bullying

Partner	P3
Author	Redial Partnership
Topic to be addressed and its definition	**Cyberbullying** can be defined as the use of electronic communication devices to bully a person. Electronic communication can include the use of computers, mobile phones, tablets and game consoles. Cyberbullying can take place through the use of emails, text messages, social networking sites such as Facebook and Twitter, chat rooms, interactive video games and many other areas too. As technology advances, more potential avenues for cyberbullying open up. Examples of cyberbullying could include posting mean, offensive or embarrassing comments or photos on social networking websites, sending threatening or abusive emails, or creating fake online profiles to embarrass or belittle another person. The different types of cyberbullying are the following: - "Threats and intimidation" - "Harassment or stalking": to follow someone, gather information and send messages repeatedly - "Defamation": to assault someone online for a behaviour that others find inappropriate in order to humiliate and embarrass them - "Peer rejection and exclusion" - "Identity theft" - "Publicly posting, sending or forwarding personal or private information or images"

	- "Trolling": to anonymously abuse someone for fun in order to frustrate or intimidate them - "Roasting": to conspire as a group in order to send or post abusive messages about a victim until the person "cracks" - "Flaming": to deliberately share content online in order to provoke someone or stir up an argument Cyberbullying is carried out online, although many victims state that they have also been bullied face-to-face, and this means that the abuse feels inescapable. As a result, the risks of cyberbullying are higher than bullying and thus the consequences are heavier on the victim.
Risk and consequences	Young people are more likely to experience cyberbullying. Potential targets for cyberbullying are generally those who are viewed as different, weak, having low self-esteem, or being lower on the social hierarchy. Youth with disabilities, people of different colours or religions, or members of the LGBTQ community can all become victims of cyberbullying. Besides, cyberbullying victims who seek revenge can end up becoming perpetrators themselves, creating a dangerous cycle. Some of the risks can be the following: - Cyberbullying can happen at any time of day. The bullies can access the internet at any time, so their behaviour is not confined to work, school or social hours. - A larger audience can be involved, even unwittingly, in cyberbullying. For example, if a bully uploads a photo of a victim to the internet, that photo can be seen and shared with a much wider audience. - Bullies can hide their identities more easily on the internet. Often known as "keyboard warriors" or "trolls", bullies are able to behave in ways that they might not in the 'real' world because their identity can be hidden. - Cyberbullies don't usually see their victims' reactions when they bully them online, which means that they are separated from the emotional distress that they cause. This is especially concerning as cyberbullies don't suffer the emotional impact their behaviour causes, which means they are less likely to stop.

	The consequences of cyberbullying can be severe and have a wide range of effects on a person: - Mentally: feeling upset, humiliated, foolish, terrified or angry - Emotionally: feeling guilty, sad or depressed, losing interest and having a low self-esteem - Physically: suffering from insomnia, headaches and stomachaches Victims may isolate themselves, be reluctant to speak up or make an effort to solve the problem if they feel mocked or harassed by others. Their behaviour can drastically change and they may resort to drugs to forget reality. Cyberbullying can, in severe circumstances, even result in suicide.
Signs to be monitored	Both the victim and the bully may show specific signs such as behavioural modifications and emotional symptoms as a result of cyberbullying. Here are the signs to monitor if you think your child may be a victim of cyberbullying: - feeling uneasy or anxious when using their phone, - being reluctant to use technological devices and not wanting to talk about their online activities, - changing their eating or sleeping patterns, - isolating/excluding themselves from friends and family, - no longer wanting to attend school or any activities outside the house - showing signs of depression, anxiety, or suicidal thoughts Here are the signs to monitor if you think your child is cyberbullying others: - becoming more discreet about their online activity, - having multiple social media profiles or accounts, - exhibiting behavioural changes at home or school, - showing personality changes, especially aggressive ones, - becoming more concerned with social status, - using their device more frequently and trying to hide their online activity on their phone or computer, - getting upset when they can't laugh at things online but don't

	want to discuss what they are. As a result, parents need to be very careful with the online activities of their children and especially monitor any changes in behaviour they may have. In particular, they should raise awareness of the risks that the internet presents and be there for their children so that they don't hide anything from them and don't isolate themselves making it harder to report any cyberbullying.
Tips to prevent the risk for families	- Engage with your children in mutual activities and communities online - Don't ignore your children or overreact if they want to talk to you or share with you information about their online activities whether it's for school or entertainment so that you may be more aware of their environment - Learn about cyberbullying and other risks in order to protect your children, raise awareness about this issue and teach them how to properly protect themselves online - Never hesitate to seek help and involve the school or other organisations if the behaviour of your children seems to worsen or starts to resemble any sort of threat.
Tips to prevent the risk for young people	- Be mindful of how you treat others and what you comment on other's posts - Block somebody in order to prevent them from seeing your profile or contacting you - Don't answer provocations and don't engage in controversial debates - If you are victim of any cyberbullying, keep and collect all the evidence online in order to easily file a complaint - Never hesitate to ask advice or seek help from someone you trust such as your parents, a close family member or another trusted adult
Technical tools	Cyberbullying mostly happens on social networks and social media where people communicate and interact the most and thus where victims are the most at risk of being bullied. Each social media site provides a variety of features that let a person choose who can access or comment on posts, join automatically as

	a friend, and report bullying incidents. A lot of them include easy procedures for blocking, muting, or reporting cyberbullying. Social media firms also offer teachers, parents, and kids educational resources and advice on how to stay safe online. As a matter of example, Facebook and Instagram provide anti-bullying tools with options to: - manage privacy settings, - block users and accounts, - mute an account and prevent notifications, - secure an account by restricting who can view and have access to it, - control, filter and delete comments, - limit direct messaging, - report a content for reasons that include, hatred, violence, nudity, fake news, bullying, abuse etc All social media platforms also prohibit the publication of inappropriate content and sort out offensive messages and comments that violate community guidelines.
Existing national and EU campaigns	Over the past decades, manifold campaigns and projects have been carried out throughout Europe to fight against cyberbullying and ensure the safety of young people online. Some of them are: Safer Internet Day: a campaign against cyberbullying launched by the European Commission in 2009 in order to empower young people to stay safe by giving them the knowledge, abilities, and resources to handle risks online. This campaign has enabled social networking businesses to sign a European agreement for child's safety online. Some of the aims are to promote safety messages, make sure services are suitable for the audience's age, give users control over their privacy settings so that their online presence is safer, provide a "report" button that is simple to use and easily reachable so that users can report offensive contact or behaviour, review illegal or prohibited content or activity. #DeleteCyberbullying: a campaign held by the European Commission from 2013 to 2014 to acknowledge the existence and danger of cyberbullying, share best practices for identifying and avoiding cyberbullying, make specific suggestions to decision-

	makers, and create online campaign materials to tackle the issue. The website from the campaign is still live and contains all multimedia products, resources and reports from the European cyberbullying conference. "European Anti-bullying Network": a conference on cyberbullying held in Athens in 2014 as part of an initiative supported by the European Commission. The conference resulted in the creation of a strong partnership between civil society organisations and authorities from around Europe that together launched the European Anti-bullying Network (EAN). The objectives are to establish alliances across Europe to coordinate anti-bullying efforts and initiatives, to have an impact on national and European policy, to create and encourage the sharing of best practices, to give field experts the tools and training they need, to educate the public about bullying and to give children, teenagers, parents, and teachers the tools they need to deal with it.
Positive narrative	"From Cyberbullying to Well-Being: A Narrative-Based Participatory Approach to Values-Oriented Design for Social Media" The purpose of this study is to create positive technologies for young people by examining cruel and harsh online behaviour. Using the study technique of a narrative inquiry, four cyberbullying stories were mapped out by two focus groups, one of which was made up of teenagers and the other of undergraduate students. Every cyberbullying narrative included two subplots: the one that "is" (as these participants saw it) and the one that "could be" (if the participants' design suggestions were implemented on social media). In the participants' cyberbullying tales, there are seven emerging design patterns that stand out: design for reluctance, design for consequence, design for empathy, design for personal empowerment, design for fear, design for attention, and design for control and repression.
Case study	Example of a case study taken from the project Joining forces to Combat Cyberbullying in Schools Ashley's education has been influenced like any other adolescent by both her parents and her friends at school. She had no idea how intrusive the Internet could be without her knowledge or even her

	having a choice in the matter. The bullying that took place in Ashley's case may have seemed harmless at first glance, but it had the potential to be far worse. Ashley was 11 years old when a classmate started taking pictures of her without her knowledge. The pictures were then put in an online informational portfolio that was published on a false social media page. The internet page was designed to make it appear as though Ashley posted everything herself. Ashley only learned about the website's existence from friends and other people. The information published was very detailed as well: it included the name of her school, her address, details about her family, her birthdays, and more. Even worse, there was no restriction applied to any of the data, it was all left wide available to the public. When confronted, the page's creator denied doing anything wrong. Meanwhile, Ashley started to experience bullying from her schoolmates. Ashley had to enrol in a different middle school to start over and get a "clean slate." The damage caused by this cyberbullying case was that she lost her friends and changed her school thus having to adapt to a whole new environment again. The consequences could have been way worse for her and her family given the fact that all her private information was available to the public and thus exposed to any harm online and offline.

3. Dangerous online challenges

Partner	P2
Author	ICEP
Topic to be addressed and its definition	**Dangerous online challenges** - An online challenge generally involves an individual recording themselves completing a challenge and distributing the video through social media channels. The challenge is often something difficult or daring, which they then invite others to complete themselves.

Risk and consequences	Dangerous online challenges in the form of dares can be incredibly dangerous precisely because they spread so quickly via social networks. Kids can suffer injuries and even die. Adults are susceptible either way.
Signs to be monitored	- Duration of time spent on social media - Contain the watched videos and status on social media - Psychological state of children - loneliness, tightness, fear, pressure
Tips to prevent the risk for families	- Create an account for children with Family Pairing - TikTok's parental controls let parents filter explicit content and set screen time limits. - Set up an account for a child (13 and under). With such accounts, commenting and direct messaging are automatically disabled, no inappropriate users will be able to comment on child content or reach out to them. - Check out the parental-control options built into ID protection services such as Norton LifeLock. That way you'll protect kids against identity theft, cyber predators, and hackers all at once. - Staying in touch on the preferred communication platforms of kids can help them keep in touch with what goes on in their day-to-day lives. Watch their stories for clues about what is going on in school and with their friends. Let the children know that if you pay for the device and the wireless network, they have to friend you in exchange. - Ask your child to 'friend' you on social media. Younger teenagers might be OK with this, but older teenagers might prefer not to friend you.
Tips to prevent the risk for young people	- Create a list of media priorities to choose from - To explain how to behave online and why it's important - Talk about upsetting and inappropriate content. If you can talk with your child in an open and non-judgmental way, they're more likely to talk with you if they come across something disturbing online or have a bad online experience.

	- Encourage and remind them to explore and use the internet safely. For example, by checking their privacy settings. - Find out how to make a complaint about offensive or illegal online content.
Technical tools	- TikTok's parental controls (restricted modes, video keyword filters, family pairing controls) https://support.tiktok.com/en/safety-hc/account-and-user-safety/user-safety - Parental-control options built into ID protection services such as Norton LifeLock https://www.nortonlifelock.com/us/en/ - Family Media Plan https://www.healthychildren.org/English/fmp/Pages/MediaPlan.aspx#/family
Existing national and EU campaigns	- https://raisingchildren.net.au/teens/entertainment-technology/cyberbullying-online-safety/internet-safety-teens - https://www.highspeedtraining.co.uk/hub/how-to-respond-to-dangerous-online-challenges/ - https://nationalonlinesafety.com/wakeupwednesday/what-you-need-to-know-about-hoaxes-and-online-challenges - https://www.security.org/news/tiktok-dangers/ - https://www.healthychildren.org/English/family-life/Media/Pages/Dangerous-Internet-Challenges.aspx
Positive narrative	How to Make a Family Media Use Plan One of the approaches to help resolve the risks connected with dangerous online challenges is to create a personalised Family Media Use Plan that works within your family's values and busy lifestyles. This interactive tool developed by the American Academy of Pediatrics (AAP) includes a Media Time Calculator that can give a snapshot of how much time each child is spending on daily activities, such as sleeping, eating, homework, physical activity, and media use. It also includes AAP recommendations on screen-free zones, media manners, and much more.
Case study	A 12-year-old boy in Aurora, Colorado has died after taking part in

	the "blackout challenge" on TikTok that calls for people to choke themselves until they become unconscious. Joshua Haileyesus was admitted to the hospital on 22 March and spent 19 days on life support. His twin brother found him passed out on the bathroom floor. https://www.independent.co.uk/news/world/americas/blackout-challenge-tiktok-dead-denver-b1831327.html A 13-year-old in Ohio has died after "he took a bunch of Benadryl," trying a dangerous TikTok challenge that's circulating online. Jacob Stevens was participating in a TikTok challenge with some friends at home when he ingested the antihistamine, the family donation account states. Jacob was on a ventilator for almost a week before he died. https://tinyurl.com/y6ppt9cw

4. Internet addiction

Partner	P4
Author	Emphasys
Topic to be addressed and its definition	**Internet addiction** can be described as excessive or poorly controlled preoccupations, urges or behavoiur when making use of any computer device and the internet access that lead to impairment or distress.
Risk and consequences	The main risks and consequences of Internet addiction are: Physical Symptoms such as: - Back or shoulder pain - Headaches - Vision problems - Insomnia - Lack of proper hygiene - Poor nutrition - Unintended weight gain or loss (PsychGuides, n.d.)

	Emotional Symptoms such as: - Anxiety - Depression - Increased irritability - Isolation - Feelings of guilt - Avoidance of work - Feelings of euphoria when using the computer (PsychGuides, n.d.)
Signs to be monitored	The signs are listed below: - No longer engaging in activities that were once enjoyable - Spending most waking hours online - Anger or agitation if you are asked to step away from your device of choice - Lying about your internet use - Concealing your internet use

Tips to prevent the risk for families	**Parents and caregivers need to be prepared** to be unpopular and provide clear boundaries for their children. Some measures that can be taken include the following: - Limit the use of TV, computers and mobile devices to a maximum of 30 minutes at a time. Ensure the total amount of screen time per day doesn't exceed the age-group recommendations. - Schedule an appropriate time for using the device, and plan fun physical activities for your child to engage in at other times. - Refrain from putting TV and electronic gadgets in your child's bedroom, and put away such devices after use. - Observe 'tech-free' times such as during meals, homework and bedtime. In addition, you can designate 'tech-free' zones for your child such as in the bedroom, dining area and car. - Teach your child early about the importance of moderation. Be sure to offer praise when your child demonstrates restraint in the use of tech devices and follows the rules you've set. - Monitor access by using the device with your child. Take this opportunity to communicate, interact and share family values.
Tips to prevent the risk for young people	- **Admit it:** The first thing that young people should do is admit it and proceed with therapy with a specialist. - **Seek Therapy:** Then, seeking therapy is important since the consequences can be heavy for young people. When sharing the emotions with someone else (especially expert) it helps in opening up. - **Limit smartphone use:** Once you have admitted that you may have internet addiction problems it's time for you to do something about it and not let it take control over your life. A

	good practice for this may be to limit the online sessions to 30 minutes. - **Socialise:** Another way to face this problem is to socialise. In order to do so, real life experiences are essential and inviting friends and engaging in different activities may be the best solution. In addition, going out more frequently and making your loved ones your priority may be helpful as well. - **Change communication patterns:** Instead of communicating with your friends by using the phone, try to change the pattern and meet them so that you talk to them face to face. - **Follow a routine:** A routine makes people more organised and helps young people be consistent with their priorities. - **Prioritise your needs:** Focus on the things you want to get done first. For students, it is really important to prioritise their needs with school responsibilities and homework to be consistent. - **Keep devices inaccessible:** If things are getting out of control and you find yourself getting more addictive day by day, fixing the time period can be helpful. Besides, you can ask for help from a friend and let him keep your things for a while to give you the necessary space. - **Be active:** There are many things that people can do to be active. Outdoor activities are the most helpful for all people, especially for young people. Young people can be a part of a sports team, volunteer programmes, civic groups, and other communities to feel worthy and spend quality time. - **Know the cause:** Find out your reason and sort out a way to resolve it. Once you know the feelings that lead you to the unnecessary use of the internet, you might be able to resolve those issues on your own.
Technical tools	1. **Medication**: The use of medications is beneficial for people who are suffering from underlying mental health conditions such as depression or anxiety and have developed internet addiction as a result. 2. **Cognitive behavioural therapy (CBT)**: A common approach to treating internet addiction is CBT. It focuses on changing negative thought patterns that trigger anxiety and produce addictive behaviours. 3. **Support groups**: People who suffer from electronic addiction can find solace in support groups that provide a safe place while reducing shame or social isolation. Internet addiction

	support groups include Internet and Technology Addicts Anonymous, Online Gamers Anonymous and Computer Gaming Addicts. 4. **Inpatient treatment program:** Residential or inpatient treatment programs involve staying in a professionally staffed facility. This means staying in a supportive environment that offers medical supervision, in which an internet addict can recover without worrying about internet usage. In addition to this, there are some **smartphone applications** that could help reduce internet use: - Freedom - YourHour - QualityTime - Lock&Stock - Social Fever - Stay Focused - Detox - Antisocial - Off The Grid - Digitox - ActionDash
Existing national and EU campaigns	- Cyprus Safer Internet Centre - CYberSafety - Safer Internet Day
Positive narrative	Although referring to the positive aspects of an addiction seems like a contradiction, the internet has many benefits and consequently, has become a part of everyday life, being used for news, information, research, communication and relationships. **1. Expanded Knowledge Base** The Internet enables people to have access to a variety of information sources from around the world which gives them the chance to conduct research and business transactions. Besides, not only can internet users conduct business transactions, for instance, but they can also access international libraries, museums among many others. What's more, many children research school projects and often use the Internet for fun, games and email. According to the authors of "Internet Applications of Type II Uses of Technology in

	Education," Internet use in schools empowers students to use technology to create their own learning environments "filled with enthusiasm and self-motivation." **2. Ease of communication** It is due to the internet that nowadays users have the ability to communicate with friends and family faster than ever thanks to email, blogs, discussion forums or even chat rooms. On the other hand, working from home via the internet has changed the way many businesses operate. **3. Relationships** While Internet addiction can harm personal relationships, the Internet can also make relationships stronger because of the ability to communicate easily.
Case study	Cyberspace – Addiction or Not As access to Internet technologies especially due to the COVID-19 pandemic has increased, so too have behavioural disorders related to Internet use. Through this case study we can recognise the importance of internet addiction for students, the consequences and the signs to be monitored.

5. Loss of privacy and scandals related to the misuse of personal data

Partner	P5
Author	Edupuntozero
Topic to be addressed and its definition	The rapid advancement of technology in recent years has raised unique privacy challenges. As people increasingly rely on digital platforms and services, they unknowingly leave behind vast amounts of personal information that can be used for purposes beyond their control. Individuals are often not fully aware of these problems because privacy is an abstract concept that originated in law essays.

	The EU, among many others, took the lead with an innovative legislation: The GDPR or General Data Protections Regulation. The regulation was put into effect on May 25, 2018. It is very important to understand privacy for both families and students. Their data is constantly under threat. Many of these threats concern their personal lives. While giving away personal data seems harmless, it has led to the widespread collection and storage of personal data that can be used for more nefarious purposes. Data breaches can expose personal information such as email addresses, passwords, and credit card numbers, leaving individuals vulnerable to identity theft and financial fraud. Private moments can be easily shared and exploited by individuals with malicious intent. Italy still remembers the tragic story of Tiziana Cantone. Moreover, scandals have emerged around the misuse of personal data by both governments and private companies. For example the 2018 Cambridge Analytica scandal revealed that personal data harvested from millions of Facebook users without their consent was used to influence the American political campaign. This raised concerns about the potential manipulation of democratic processes through the use of personal data.
Risk and consequences	High school students are particularly vulnerable to loss of privacy and data misuse due to their frequent use of social media and other digital platforms. - Online abusers may use personal information provided by students for trolling or other forms of exploitation. - Another risk that students may face is the loss of control over their data, which can include private information or moments that can be spread on the internet without their knowledge. This loss of control can be caused by various factors such as data breaches, hacking, or intentionally sharing information with others who then share it without consent. - Students often don't have enough tools to understand the

	potential harm that information can do to them and how they are sacrificing their own privacy. - In some cases, schools and educational institutions may use data analytics to monitor student behaviour and academic performance, potentially leading to concerns about privacy and discrimination. - High school students should be cautious about what personal information they share online and consider using privacy settings to limit access to their profiles. - Students should also be careful about clicking on links or downloading attachments from unknown sources, as these could contain malware or viruses that could compromise their personal data.
Signs to be monitored	There are several signs you can monitor to help protect your information. Here are some common signs to watch for: - Unexpected emails, text messages, or phone calls asking for personal information, such as your name, address or credit card number. Unsolicited requests for personal data may be a phishing attempt to steal your information. - Notifications or emails from your social media or email accounts indicating that your account has been accessed from an unfamiliar location or device. This could be a sign that someone has gained unauthorised access to your account. - You receive suspect messages from your friends or your parents asking for data. Their accounts or devices may have been compromised. - Your personal data may have been compromised in a data breach. In this case, it's important to take steps to protect your information, such as changing your passwords and monitoring your accounts for suspicious activity.
Tips to prevent the risk for families	- Encourage your family members to enable two-factor authentication on all their accounts. This adds an extra layer of security and can help prevent unauthorised access to their accounts. - Install antivirus software on your family devices.

Tips to prevent the risk for young people	- Think carefully before you post something online, and ask yourself if you would be comfortable with anyone seeing it. Remember that things you post online can be seen by anyone, including potential employers or college admissions officers. - Enable two-factor authentication on all your accounts whenever possible. This adds an extra layer of security and can help prevent unauthorised access to your accounts. - Be cautious when downloading apps or games, and make sure you understand what information they are collecting and how it will be used. Android and IOS smartphones have privacy settings for every app, allowing users to restrict some types of data. - Be careful who you chat with: Be careful about who you chat with online and don't share personal information with strangers. Remember that not everyone online is who they say they are.
Technical tools	- A VPN (Virtual Private Network) is a tool that can help protect your privacy by encrypting your internet traffic and masking your IP address, making it more difficult for others to track your online activity. Like ProtonVPN, TunnelBear and others. - Ad-blockers can help protect your privacy by blocking ads and pop-ups that could potentially contain malware or spyware. - Antivirus software can help protect your devices from malware and viruses that could potentially compromise your personal data. Like Avast or AVG. - Password managers can help you create and store strong, unique passwords for each of your online accounts, making it easier to protect your personal data from hackers. Like 1Password, Last Pass or Bitworden. - Two-factor authentication (2FA) adds an extra layer of security to your online accounts by requiring a second form of verification, such as a code sent to your phone or email address. Like Google authenticator, Microsoft Authenticator, Authy. - Privacy-focused web browsers: Privacy-focused web

	browsers, such as Tor and Brave, help protect your privacy by blocking tracking cookies and masking your IP address.
Existing national and EU campaigns	Finalmente un po' di Privacy (Finally a bit of privacy) The institutional communication campaign of the Italian Garante starts to raise awareness among citizens and consumers about the importance of protecting personal data.
Positive narrative	In today's digital age, there are many positive aspects to the use of technology and the internet. Online platforms and social media have brought people closer together, making it easier to connect with friends and family members, even if they are far away. The internet has also provided us with access to an incredible amount of information, which can be incredibly helpful for learning, research, and personal growth. Furthermore, technology has opened up new avenues for creativity, with platforms such as YouTube, TikTok, and Instagram providing opportunities for individuals to express themselves and share their talents with the world. These platforms have even provided opportunities for young people to become entrepreneurs and build successful careers, showcasing their skills and creativity to a wide audience. In addition, technology has enabled us to be more efficient and productive, allowing us to complete tasks and communicate with others more easily and quickly. It has even enabled us to work remotely, giving us more flexibility in how and where we work. While it's important to be aware of the risks and potential drawbacks of using technology and the internet, it's also important to recognise the positive impact that these tools can have on our lives. By using technology responsibly and taking necessary precautions, we can enjoy the many benefits that the digital world has to offer.
Case study	In 2010, Cambridge Analytica, a British consulting firm, gathered personal data from millions of Facebook users without their consent, primarily for political advertising. This event probably influenced the result of the American political election.

	More: MIT - Facebook/Cambridge Analytica: Privacy lessons and a way forward

6. Web-tracking

Partner	P1
Author	PROMIMPRESA SOCIETA' BENEFIT SRL
Topic to be addressed and its definition	**Web tracking** is a practice that involves collecting data on a user's browsing activity while they are online. This data is used to monitor and analyse user behaviour, preferences, and interests, with the aim of providing more personalised and targeted advertisements, improving website design, and developing more effective marketing campaigns.
Risk and consequences	While web tracking can be beneficial for businesses and advertisers, it can also pose risks and consequences for young people. One of the main risks associated with web tracking for young people is the potential loss of privacy. As web tracking technologies become more sophisticated, they can collect increasingly detailed and personal information about users. This can include information such as a user's location, interests, and online behaviour patterns. For young people, who are often less aware of the risks associated with online activity, this can be particularly problematic. Web tracking can expose young people to unwanted attention, targeted marketing, and potential exploitation. Another risk associated with web tracking is the potential for data breaches and identity theft. The data collected by web trackers can be used by malicious actors to steal a user's identity, access their personal accounts, or engage in other criminal activities. Young people, who may be less familiar with online security best practices, can be particularly vulnerable to these risks. In addition to these risks, web tracking can also have a range of

	negative consequences for young people. For example, it can contribute to the development of addictive behaviours around social media and online activity, leading to increased levels of anxiety, depression, and other mental health problems. Web tracking can also contribute to the spread of disinformation and fake news, which can have serious consequences for young people's understanding of the world around them.
Signs to be monitored	To mitigate the risks associated with web tracking, it is important for parents, educators, and young people themselves to take steps to monitor and limit their online activity. One important step is to use ad-blocking software or privacy-focused web browsers, which can help limit the amount of data collected by web trackers. Parents and educators can also help young people understand the risks associated with web tracking and develop healthy online habits. There are a number of signs that parents and educators can look out for to monitor young people's online activity and identify potential risks associated with web tracking. Some key signs to watch for include changes in behaviour, such as increased levels of anxiety or withdrawal from social activities, changes in sleep patterns, and a decrease in academic performance. Other signs can include changes in online activity patterns, such as increased time spent on social media, changes in the types of websites visited, and an increase in the number of pop-up ads or other online distractions.
Tips to prevent the risk for families	In addition to monitoring online activity and identifying potential risks, parents and educators can also take steps to help young people develop healthy online habits. This can include setting clear guidelines around online activity, encouraging young people to take regular breaks from screens, and promoting the use of offline activities and social interactions. By taking a proactive approach to online activity and monitoring, parents and educators can help protect young people from the risks associated with web tracking and promote healthy digital habits that will serve them well into the future. As a parent, there are several steps you can take to help prevent the risks of web tracking for your child. Here are some tips:

	- Install ad-blocking software: Install ad-blocking software on your child's devices to prevent targeted ads and trackers from displaying on their screens. This can help limit the amount of data that is collected about your child's online activity. - Use a VPN: Consider using a Virtual Private Network (VPN) to help protect your child's online privacy. A VPN creates a secure connection to the internet and masks your child's IP address, making it harder for trackers to collect their data. - Monitor your child's online activity: Keep an eye on your child's online activity and talk to them about any concerns you may have. Use parental control software to limit their access to certain websites or online activities that you deem inappropriate or potentially risky. By taking these steps, you can help protect your child's online privacy and reduce the risks associated with web tracking. Remember to talk openly with your child about the importance of online privacy and security, and encourage them to be vigilant and cautious when using the internet.
Tips to prevent the risk for young people	As for parents and educators, there are many tips that this manual wants to address to all young people. Besides being mindful of online activities and recognising potential risks, there are steps you can take to develop healthy habits in the digital world. Consider the following tips: - Set clear guidelines: Establish clear guidelines for your online activities. This includes how much time you spend online, the websites and apps you use, and the information you share. Having these guidelines in place will help you navigate the online world responsibly. - Take regular breaks: It's important to give yourself regular breaks from screens. Spending excessive time online can negatively impact your well-being and productivity. Make sure to engage in offline activities like hobbies, sports, and spending time with friends and family. - Prioritise offline activities: While the internet offers a wealth of information and entertainment, don't forget about the value of offline activities. Read books, pursue creative projects, and engage in face-to-face interactions. This balance will contribute to a healthier lifestyle overall.

	- Consider ad-blocking software: Install ad-blocking software on your devices to prevent targeted ads and trackers from collecting your data. This will give you more control over the information that is collected about your online activities. - Employ a VPN: Explore the use of a Virtual Private Network (VPN) to enhance your online privacy. A VPN creates a secure connection and encrypts your data, making it harder for trackers to collect your information. - Communicate with trusted adults: Maintain open lines of communication with your parents, guardians, or educators. Discuss any concerns or questions you may have about your online activities. They can provide guidance and support to help you navigate the digital world safely. By following these tips, young people can protect their online privacy and reduce the risks associated with web tracking. It's crucial to stay informed, make responsible choices, and prioritise well-being when engaging with the online world.
Technical tools	Here are some technical tools that can be used to help prevent web tracking for young people: 1. Privacy-focused web browsers: As mentioned earlier, using privacy-focused web browsers such as Brave, Mozilla Firefox with enhanced tracking protection, and Tor can help block third-party trackers and prevent websites from collecting data about online activity. 2. Ad-blockers: Installing ad-blockers on devices can help prevent targeted ads and trackers from displaying on screens. This can limit the amount of data that is collected about online activity. 3. Virtual Private Networks (VPNs): VPNs can create a secure connection to the internet and mask IP addresses, making it harder for trackers to collect data. 4. Anti-tracking browser extensions: There are several browser extensions that can block trackers, such as Privacy Badger, uBlock Origin, and Ghostery. 5. DNS resolvers: DNS resolvers, such as Cloudflare's 1.1.1.1 and Google's Public DNS, can encrypt DNS requests and prevent internet service providers from tracking online activity.

	6. Privacy-focused search engines: Using privacy-focused search engines such as DuckDuckGo or StartPage can prevent search engines from collecting data about online searches. 7. Password managers: Password managers can help young people create strong and unique passwords for their online accounts and prevent the reuse of passwords across multiple accounts. While technical tools can be helpful, it's important to remember that they are not foolproof and should be used in conjunction with other preventative measures such as education, monitoring online activity, and limiting social media use.
Existing national and EU campaigns	Italy has implemented several privacy regulations in recent years, including the General Data Protection Regulation (GDPR), which requires companies to obtain explicit consent from individuals before collecting and processing their personal data. The Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) has also issued guidelines on online profiling and cookies, which aim to protect individuals' privacy online. Additionally, some non-profit organisations and advocacy groups in Italy have focused on educating the public about online privacy and the risks of web tracking. For example, the Electronic Frontier Foundation (EFF) has an Italian language website that provides resources and information on privacy and digital rights. It's important to note that while national campaigns can be helpful in raising awareness about web tracking and other online privacy issues, individuals and families can also take proactive steps to protect their online privacy and security, as outlined in the previous responses.
Positive narrative	While web tracking can have potential risks and negative consequences for online privacy, it's important to acknowledge that there are some positive aspects of web tracking as well. For example: - Personalised online experiences: Web tracking allows

	websites to gather data about users' browsing habits and preferences, which can be used to provide more personalised online experiences. For example, a shopping website may use data about a user's past purchases to recommend similar products or offer personalised discounts. - Improved advertising: Web tracking allows advertisers to target their ads more effectively to users who may be interested in their products or services, which can improve the overall advertising experience. This can benefit both users, who may be more likely to see ads that are relevant to them, and advertisers, who can see improved conversion rates. - Improved website performance: Web tracking can provide website owners with valuable insights into how users interact with their website, which can be used to improve website performance and user experience. For example, website owners can use data about users' click-through rates and time spent on certain pages to optimise website layout and design. - Research and analytics: Web tracking can also be used for research and analytics purposes, such as tracking the effectiveness of marketing campaigns or measuring user engagement with online content. This data can be valuable for businesses and organisations looking to improve their online presence and reach. It's important to note that these positive aspects of web tracking should be balanced with considerations for online privacy and data security. While web tracking can provide benefits, it's essential to ensure that user data is collected and used ethically and transparently, with appropriate measures in place to protect users' privacy and security.
Case study	Source: https://www.eff.org/wp/school-issued-devices-and-student-privacy For the past two years, the Electronic Frontier Foundation (EFF) has been investigating the privacy implications of educational technology services. What they've found is that many of these services collect more information than is necessary, and they

	store this data indefinitely. This data can go beyond simple personally identifying information (PII) like a student's name and date of birth, and can include things like browsing history, search terms, location data, contact lists, and even behavioural information. The concerning part is that some programs automatically upload this student data to the cloud, without the awareness or consent of students or their families. This means that technology providers may be gathering information about students without their knowledge or permission, and school districts may be unwittingly assisting them. Since 2015, the EFF has been investigating how educational technology companies are protecting students' privacy and data. They have compiled their findings in a paper that aims to bring attention to the problems and issues around student privacy, and provide concrete steps that stakeholders including teachers, parents, students, and administrators can take to advocate for student privacy in their communities. As a teacher, it's important to be aware of the potential privacy implications of the technology and services you use with your students. Consider researching and reviewing the privacy policies of any educational technology you use in your classroom, and advocate for clear and transparent policies that respect student privacy.

7. Spreading of fake news

Partner	P5
Author	Edupuntozero
Topic to be addressed and its definition	The spread of **fake news** has become a major issue in today's society. With the rise of social media and the internet, false information can now reach millions of people within seconds,

	often leading to harmful consequences. Fake news is defined as news stories with false or misleading information, deliberately created to disinform. This can range from completely false stories to partially true stories with significant omissions or twists. The spread of fake news is often motivated by political or financial gain, as well as the desire for attention and fame. One of the main reasons why fake news spreads so quickly is that people tend to share information without fact-checking it first. Social media platforms, which often prioritise engagement and virality over accuracy, also contribute to the rapid spread of fake news. The consequences of fake news can be significant. It can influence public opinion, shape political outcomes, and even incite violence. For example, false information about the safety and efficacy of vaccines has led to decreased vaccination rates during Covid-19 in the US and EU. To combat the spread of fake news, it is important for individuals to be critical consumers of information. This means fact-checking stories before sharing them, looking for multiple sources, and being wary of clickbait headlines. It is also important for social media platforms and news organisations to prioritise accuracy and transparency over engagement and clicks.
Risk and consequences	- **Misinformation** - The spread of fake news can lead to the dissemination of misinformation, which can mislead individuals and create confusion. This can have serious consequences, particularly in areas such as health, where misinformation can lead to harmful behaviour and decisions. - **Damaged reputations** - Fake news can damage the reputations of individuals and organisations. False accusations or negative stories can damage political figures and change election results. - **Polarisation** - Fake news can contribute to political

	polarisation by promoting extreme or misleading views. This can make it more difficult for people to engage in productive dialogue and compromise, leading to increased tensions and division. - **Violence** - Fake news can contribute to violence, particularly in situations where it is used to incite hatred or inflame tensions. For example, fake news stories about religious or ethnic groups can lead to violent attacks and discrimination. - **Undermined trust** - The spread of fake news can undermine trust in institutions and media sources, which can have long-term consequences for democracy and public discourse.
Signs to be monitored	- The awareness of sources that are not reputable, such as anonymous blogs or social media accounts. These sources may not be held to the same standards of accuracy and verification as established news outlets. - Fake news related to emotions and sensationalises events in order to gather attention. If a story seems too good (or bad) to be true, it may be worth fact-checking before sharing. - It is always a good idea to verify information by checking multiple sources. If a story is not corroborated by other reputable sources, it may be a red flag. - Fake news often uses misleading or inaccurate information in order to promote a certain narrative. Be on the lookout for stories that cherry-pick facts or statistics in order to support a particular viewpoint.
Tips to prevent the risk for families	- Encourage your family members to think critically before accepting information as true. - Teach your family members about reputable and reliable sources of news. Introduce them to established news outlets. - Make fact-checking a family activity. Encourage everyone to fact-check information before accepting it

	as true or sharing it with others. - Talk about media bias and the importance of being aware of different biases in news reporting. Teach your family members to recognise and interpret bias in news articles, headlines, and social media posts. - Encourage the use of multiple sources and explore diverse viewpoints. - Teach your family members to be responsible when sharing information. Encourage them to think critically, fact-check, and consider the potential impact of sharing false or misleading information.
Tips to prevent the risk for young people	- Check the credibility of the source before reading or sharing any news. - Use multiple sources to verify the information. Compare sources and consider whether they agree on key facts or present different perspectives on the same event. - Be aware of when an article was published. Some fake news stories are outdated or recycled stories that are presented as current events. - Clickbait headlines are designed to attract attention and entice people to click on a story. Be aware of sensational headlines and check the credibility of the source before clicking. - Be aware of your own biases and assumptions. Question whether you are interpreting information in a way that supports your pre-existing beliefs or opinions.
Technical tools	1. Fact-checking websites: Fact-checking websites such as Snopes, FactCheck.org, Washington Post Fact Checking, Politifact, Reuters Fact Checking can help verify the accuracy of information. These sites provide a wealth of information on a wide range of topics, and can help debunk false claims and rumours. 2. Browser extensions: Browser extensions like NewsGuard and Factmata can help to identify fake news and misinformation. These extensions use algorithms to analyse websites and flag potentially misleading content. 3. Social media tools: Social media platforms like Facebook

	and Twitter have introduced features to help combat fake news and misinformation. These features include fact-checking labels and warning messages that alert users to potentially misleading content (Meta Transparency Center) 4. Machine learning algorithms: Machine learning algorithms can be used to detect patterns in the spread of fake news and misinformation. These algorithms can help to identify sources of fake news and to predict where misinformation is likely to spread. 5. Image verification tools: Image verification tools like Google's Reverse Image Search can help to identify whether an image has been edited or manipulated. This can be especially useful for identifying fake news stories that use doctored images to support false claims.
Existing national and EU campaigns	From the official website: "EUVSDISINFO is the flagship project of the European External Action Service's East StratCom Task Force (opens in a new tab). It was established in 2015 to better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the shared neighbourhood. EUvsDisinfo's core objective is to increase public awareness and understanding of the Kremlin's disinformation operations, and to help citizens in Europe and beyond develop resistance to digital information and media manipulation".
Positive narrative	People and organisations around the world are taking action to combat the spread of fake news and promote media literacy. Here are some examples of positive narratives: 1. As awareness of the issue grows, more people are becoming educated about how to identify fake news and misinformation. Schools and universities are introducing media literacy programs, and many organisations are offering training sessions to help people develop critical thinking skills. 2. Fact-checking initiatives are gaining momentum. These organisations work to verify the accuracy of information and debunk false claims. 3. Social media platforms are taking steps to combat fake

	news and misinformation. Facebook, for example, has introduced fact-checking labels and warning messages that alert users to potentially misleading content. Twitter has introduced warning messages and has also started flagging tweets that contain manipulated media. 4. Governments and organisations are launching public awareness campaigns to educate people about the dangers of fake news and misinformation. These campaigns emphasise the importance of critical thinking and encourage people to fact-check information before sharing it. 5. There is a growing movement towards collaboration between media organisations, fact-checking initiatives, and tech companies to combat fake news and misinformation. By working together, these organisations can share resources and expertise, and develop more effective strategies to combat the spread of fake news.
Case study	During the COVID-19 pandemic, the spread of fake news has posed a significant challenge. The spread of misinformation and disinformation has exacerbated the challenges faced during this unprecedented time, impacting public health, trust in institutions, and social cohesion. The pandemic created what has been referred to as an "infodemic", an overwhelming amount of information, including false claims, spreading rapidly through various channels. False claims about cures and the origins of the virus have misled individuals, leading to vaccine hesitancy, impacting vaccination efforts and prolonging the pandemic. Social media platforms have played a pivotal role in amplifying fake news, allowing it to reach vast audiences quickly. The lack of stringent fact-checking measures and algorithms that prioritise engagement over accuracy have contributed to the virality of misinformation. Conflicting narratives and conspiracy theories have sown doubt among the public, making it harder for individuals to make informed decisions and follow public health guidelines.

	The battle against COVID-19 extends beyond medical advancements; it requires combating the "infodemic" of fake news. Educating the public about media literacy, promoting fact-checking initiatives, and fostering responsible media consumption are vital. Fact-checking organisations and initiatives have been crucial in debunking false information and providing accurate updates. These efforts have helped to counteract the spread of fake news and provide reliable information to the public. By collectively addressing the spread of fake news, we can protect public health, rebuild trust, and pave the way for a more resilient and informed society in the face of future challenges.

8. Image-based abuse

Partner	P4
Author	Emphasys
Topic to be addressed and its definition	**Image based abuse** can be described as the fact that someone shares, or threatens to share, intimate images without the consent of the person in the photo.
Risk and consequences	The risks and consequences of image-based abuse are: - Anger - Humiliation - Embarrassment - Social isolation - Worry and/or fear for their safety
Signs to be monitored	- Lack of self esteem - Lack of mental health - Lack of physical well being - Loss of confidence - Depression - Sense of social isolation

Tips to prevent the risk for families	- Avoid taking an overly negative and disciplinary approach to your child's technology use - Be non-judgemental and supportive of your child's online activities - Initiate open conversations with your child about sending nude images - Support your child's understanding of consent, bodily autonomy, equality and ethical decision making
Tips to prevent the risk for young people	- Be careful with offers or deals for 'easy money' especially on the Internet - Be suspicious if someone you don't know randomly contacts you online - If you do become an intimate content creator, take steps to protect your personal information and identity so scammers can't threaten to expose you by not using your real name and not showing your face
Technical tools	As far as technical tools are concerned, there are several examples such as the following that may help you not be an image based abuse victim: - Saasyan Safe Image AI - StopNCII.org supporting service - Garbo search engine - Pimeyes AI search engine
Existing national and EU campaigns	- Cyprus National Sexual Assault Helplines - International Women's Day 2022: EU-wide rules to combat violence against women and domestic violence - Combating gender-based violence: cyberviolence (2022/C 251/01)
Positive narrative	Some of the positive impacts of image-based abuse is: - Kids/Young people are becoming more suspicious - Young people are learning who to trust - The relationship between family members is getting stronger

Case study	Image-based abuse is sometimes called 'revenge porn' because some people do it to hurt a person who has ended a relationship with them, or threaten to do it unless they stay together. Image-based abuse existed long before the internet era. In 1953, nude images of Marilyn Monroe were published on the cover of Playboy without her consent, and every decade since high-profile women have been victimised (Grasso, 2017; Hills, 2017). With advances in AI technology in the 2010s, users no longer need real images of their victims. Instead, they can create "deep fakes." Due to the Covid-19 pandemic, stress, unemployment and confinement, a lot of people started to be addicted to digital technologies and all contributed to a significant increase in violence against women, a concurrent increase in online sexual harassment and image-based sexual abuse (UN Women, 2020; Goldstein, 2020; Taddeo, 2020; Robinson et al., 2020). In the United Kingdom, the Revenge Porn Helpline experienced a 98% increase in cases in April 2020, compared with April 2019.

9. Sexting

Partner	P2
Author	ICEP
Topic to be addressed and its definition	**Sexting** is the act of sending sexual text messages (the word is a combination of sex and texting). It often also involves sending nude or seminude photos and explicit videos of yourself.
Risk and consequences	It is illegal to send an adult message or nude to someone without their consent then so might face legal consequences in the future, exchanging sexts with a minor (less than 18 years) is considered child pornography. It is also illegal to send and receive are both illegal for minors. In addition, sexting can be viral and be used to defame people, harass and bully them too. People might suffer mentally.
Signs to be monitored	- Lot of time spent on social media - Making videos and photos

	- Posting and sending half naked photos on social media - Hiding mobile phones and messages
Tips to prevent the risk for families	-
Tips to prevent the risk for young people	- Give kids age-approximate examples by parents. - Teach teens to avoid Peer pressure for sexting - Make kids learn about state Laws. - Warn kids about the serious Consequences
Technical tools	Parental Controls On Teens' & Minors' Smartphones & Social Media
Existing national and EU campaigns	Germany: https://www.safer-sexting.de/ https://www.amberalert.eu/campaigns/think-before-you-share Netherlands: https://www.whatdesigncando.com/project/safe-sexting/
Positive narrative	Movies are made to show how dangerous the issue can be, for example one movie called Sexting in Suburbia from 2012 speaks about a mother who starts looking for an answer when her daughter Dina commits suicide.
Case study	A 16-year-old boy named Channing died by suicide after his intimate messages to another boy were made public. Private, intimate messages that Channing had shared with another boy were somehow leaked and posted on Instagram and Snapchat. He discovered them late at night on Sept. 22, and by the morning of Sept. 23 in 2019, he was dead. His father went to check on him around 4 a.m. and discovered his body. He couldn't face the humiliation of cyberbullying so he chose to commit suicide.

Mapping of local, national and international support services

1. Italy

LOCAL (NORTH OF ITALY)

1. **"SMARTBUS LOMBARDIA"**

The SmartBus is a project by Huawei and Parole O_Stili that will offer free training sessions to over 400 middle school students in order to promote a suitable level of personal awareness on the topic of internet security and the opportunities and risks associated with the use of digital tools. For students, the "lessons" are scheduled in the morning. In the afternoon of the same days, the mobile classroom will welcome citizens who wish to improve their knowledge on the topics of cybersecurity, privacy, and the use of digital tools, with evaluation tests of their level of awareness and training paths similar to those offered to schools but reworked for adult users.

The project is sponsored by the Lombardy Region, the Municipality of Bergamo, and the industry association Asstel. The SmartBus is an interactive mobile classroom equipped with digital devices that will make stops in 15 cities across 5 regions, involving over 4,500 students who can take part in educational moments through the special educational app entirely developed by Parole O_Stili for the project. Under the motto #CYBERSICURIABORDO, the program aims to make students more aware of the various protective measures to be adopted to protect themselves online, such as the use of antivirus software, updating devices, choosing complex passwords, and configuring social networks to maximise data privacy.

2. **"SCUOLA DIGITAL SMART"**

With "Scuola Digital Smart" the Lombardy Region aims to promote the creation of environments equipped with advanced technological resources and digital devices capable of integrating the use of innovative tools into education.

These are appropriately equipped and connected spaces and environments, in order to facilitate access to technologies and educational resources that are as open as possible and encourage the sharing of information, active and collaborative learning modes, and the development and expression of creativity through innovative teaching methodologies.

In addition to the application for facilitation, the interventions of the municipalities must also provide a training program for teachers and school staff involved and responsible for the use of tools and spaces, as well as a specific description of innovative teaching methodologies and activities."

3. "CULTURA E DIGITALE: NUOVE PROFESSIONI PER IL FUTURO"

Under the "Lombardia Plus - Linea Alta Formazione Cultura" call for proposals, the Enaip Lombardia Foundation ranked first with the project "Culture and Digital: New Professions for the Future", which provides for the activation of 7 free training courses:

- Cultural event organisation - Milan
- Cultural and multimedia design - Milan
- Organisation and management of events for cultural tourism
- Europroject and fundraising for culture - Milan
- Social Media Manager, SEO and SEM for culture
- Management and movement of cultural heritage
- Digital technologies for culture: web and multimedia apps

The courses are funded by the European Social Fund and are intended for unemployed individuals who are residents or domiciled in Lombardy, and who hold a high school diploma, are university students, have completed a three-year or five-year vocational diploma, or have obtained a bachelor's or master's degree.

4. PLATFORM "BULLISMO E CYBERBULLISMO LOMBARDIA"

This is a platform promoted by the School Office for Lombardy for managing preventive and intervention actions against bullying/cyberbullying in the region.

For years, the Lombardy Regional School Office has been working within the framework of Regional Law No. 1/2017 and National Law No. 71/2017 to ensure that the prevention and combating of bullying/cyberbullying in schools are aspects that are part of regular curricular programming and planning, supported by networks that involve all the forces that deal with bullying and cyberbullying, with different roles and competencies, in the territory.

LOCAL (CENTRAL ITALY)

1. LEGAL HACKERS ROMA

Legal Hackers Roma is a movement of lawyers, policymakers, designers, technologists, and academics who explore and develop creative solutions to some of the most pressing issues at the intersection of law and technology. Through local meetups, hackathons, and workshops, Legal Hackers spot issues and opportunities where technology can improve and inform the practice of law and where law, legal practice, and policy can adapt to rapidly changing technology. Legal Hackers Roma organises events, workshops, and meetups that delve into various aspects of privacy and digital issues.

These events serve as platforms for exchanging ideas, exploring emerging trends, and raising awareness about the legal and ethical challenges posed by advancements in technology. They cover topics such as data protection, cybersecurity, surveillance, encryption, online rights, and digital ethics.

NATIONAL

1. **"PROGRAMMA IL FUTURO"**

The CINI - National Inter University Consortium for Computer Science, has launched the "Programma il Futuro" project, in collaboration with the MIM - Ministry of Education and Merit, starting with the 2014-15 school year and still ongoing. The aim is to provide schools with a series of simple, effective, and easily accessible tools to train students in the basic concepts of computer science. Italy is one of the first countries in the world to experiment with the structural introduction of basic computer science concepts through programming in schools, using user-friendly tools that do not require advanced computer skills. At the beginning of each school year, the MIM invites schools to participate in the project.

2. **MIUR: "PROMOZIONE DI INIZIATIVE VOLTE A POTENZIARE LA CULTURA DIGITALE DEGLI STUDENTI"**

Digital citizenship, the challenges and opportunities of technological evolution, cybersecurity, and the promotion of responsible behaviour online. These are the topics that will be addressed in a free course aimed at fifth-grade students in secondary schools. The course, which will be held in e-learning mode, is part of the Memorandum of Understanding "Promotion of initiatives aimed at enhancing the digital culture of students" signed between the Ministry, UnionCamere, and InfoCamere with the aim of educating girls and boys on the proper use of the Internet and digital tools. Students who attend the course and pass the final test will be issued a certificate.

3. **CYBERCRIME UNIT OF THE POLICE FORCE**

The Postal and Communications Police is a specialised police force in the prevention and fight against cybercrimes, protection of privacy, and communication security. The activities of the Postal Police include:

- Investigations into cyber crimes such as data theft, online fraud, and computer scams
- Monitoring and control of online content to prevent cyberbullying, online pedophilia, and terrorism
- Protection of personal and corporate privacy in the digital sphere

- Control and suppression of email-related crimes such as spamming and phishing
- Collaborative investigations with other organisations such as Interpol and Europol in the fight against transnational cybercrime.

The Postal and Communications Police carries out several educational projects for young people and holds training days in schools, with the aim of promoting a culture of legality and cybersecurity.

4. PLATFORM "ELISA"

The ELISA platform has been designed to equip schools and educators with an array of effective tools to tackle the problem of bullying and cyberbullying. In order to achieve this objective, two specific actions have been developed. These measures, namely e-learning training and monitoring, are provided completely free of charge to all participants.

E-learning training is aimed at teachers and school principals who are responsible for addressing bullying and cyberbullying. The training includes e-learning courses to promote psycho-educational and social knowledge and skills for preventing youth distress.

The online monitoring system aims to conduct periodic studies of significant public interest aimed at schools across the national territory. It allows for the assessment, on a large scale and through anonymous questionnaires, of the presence and trends of bullying and cyberbullying phenomena in Italian schools. Moreover, the monitoring system provides individual schools with a personalised report that allows them to have a snapshot of their institution's situation regarding these phenomena and monitor their trends over time.

5. GIOVANI AMBASCIATORI PER LA CITTADINANZA DIGITALE

Giovani Ambasciatori per la cittadinanza digitale aims to create greater awareness about issues related to the improper use of the internet, emphasising fake news and cyber risks. The project involves the training of 1,250 "Young Ambassadors for Digital Citizenship," who will serve as a reference point for training and reporting for their peers within their respective institutions. The students will play a leading role in promoting the correct use of the internet.

6. FESTIVAL INTERNAZIONALE DEL GIORNALISMO

Festival Internazionale del Giornalismo in Perugia is a prominent annual event that gathers journalists, media professionals, experts, and enthusiasts from around the world.

Held in the picturesque city of Perugia, Italy, the festival serves as a vibrant platform for discussing and exploring the evolving landscape of journalism. Renowned journalists and media personalities headline the festival, sharing their experiences, insights, and expertise with the audience. They tackle pressing issues such as fake news, media literacy, press freedom, investigative reporting, and the challenges posed by the digital era.

7. AGENZIA GIORNALISTICA ITALIANA (AGI)

Agenzia Giornalistica Italiana (AGI) is an Italian news agency that plays a significant role in fact-checking and debunking misinformation. With a strong commitment to providing accurate and reliable information, AGI actively engages in fact-checking initiatives to counter the spread of fake news and ensure the dissemination of truthful content.

AGI's fact-checking efforts involve a rigorous and systematic process of verifying claims, statements, and news articles. They employ a team of experienced journalists and researchers who meticulously analyse information, cross-reference sources, and consult experts to separate facts from fiction.

8. PAGELLA POLITICA

PagellaPolitica.it is an Italian fact-checking organisation that focuses specifically on political claims, statements, and speeches made by politicians and public figures. Committed to promoting transparency and accuracy in political discourse, PagellaPolitica.it plays a crucial role in debunking misinformation, verifying facts, and holding politicians accountable for their statements.

2. Slovakia

LOCAL

1. SCHOOL PSYCHOLOGISTS

In Slovakia according to the law N°138/2019 Coll. there are **school psychologists** (which have to be in all schools) who performs psychological diagnostics, provide individual, group or collective psychological counselling, prevention and intervention to children and pupils with a focus on education and training, provide psychological counselling to legal representatives, pedagogical staff and professional staff, cooperate in overcoming barriers in the education and training of children and pupils, provide assistance to the psychologist.

NATIONAL

1. **IPčKO.SK - INTERNETOVá PORADňA PRE MLADýCH Ľ'UDí** (Internet counselling for young people)

Professional organisations help with the peer-to-peer effect, helping young people in difficulty since 2012, 24 hours a day / 7 days a week have been available free of charge, anonymously, accessible and professionally. Psychologists and social workers who devote their free time to young people who find themselves in difficult, often crisis situations. They provide them with accessible support, acceptance and professional help in a safe and anonymous environment. The story behind the creation of the IP is one where young psychologists realised that the online world was the place to reach out to young people and help them if they needed it. Research confirms that people's behaviour in the online space brings more openness and a 'loss' of natural inhibitions, and it is good and useful to use these facts in psychological intervention. To help people with difficulties, we have developed a comprehensive set of tools in both online and offline spaces that we are constantly innovating and developing.

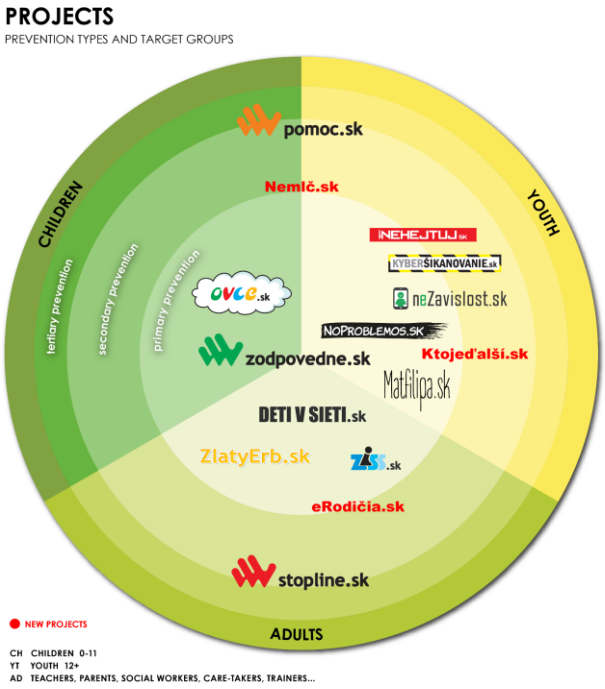
2. **KYBERSIKANOVANIE (Cyberbullying)**

Educational-musical tour for free organised by NGO eSlovensko with a series of interactive lectures with audiovisual and musical elements on the topic of cyberbullying throughout Slovakia.

3. **ZODPOVEDNE (Responsibly)**

Zodpovedne project was launched in 2007 and focuses on the safe and responsible use of the internet, mobile phones and new technologies. In this area, it focuses on raising awareness, spreading education and preventing crime in the world of children and young people. It is the only project in Slovakia supported by the European Union within the framework of the Safe Internet Community Programme.

Other projects under **the zodpovedne.sk :**



4. **POMOC.SK** Združená linka pomoci **(United Helpline)**

The aim of Pomoc is to provide coordinated help and advice for the responsible use of the internet, mobile communication and new technologies.
Online help: potrebujem@pomoc.sk

3. Cyprus

LOCAL

1. **ELECTRA**

ElectrA is a recognised NGO that provides information and support for dealing with problematic internet use.

NATIONAL

1. **CYPRUS SAFER INTERNET CENTRE**

CYberSafety is a project that aims to strengthen efforts for the creative and safe use of the internet in Cyprus. Focusing on the new and increasing needs that constantly rise, at the national and European level, regarding internet technology, the centre promotes cooperation between national stakeholders, aiming to create a safe internet culture.

2. INTERNET SAFETY

Internet Safety is an open line from the Pedagogical Institute of Cyprus aiming to inform and raise awareness, regarding the safe and responsible use of the Internet among teachers.

3. SYSTEMIC INSTITUTE CYPRUS

Systemic Institute Cyprus offers training opportunities and therapy regarding the addictive aspects of the internet. The Institute is a full member of the Training Centers of the European Association of Family Therapy (EFTA-TIC) and an approved Training Center of the European Association of Psychotherapy (EAP).

4. Ireland

LOCAL

1. "DCU ANTI BULLYING CENTRE"

To assist young people in staying safe online and to support parents and educators who may be concerned, the Anti Bullying Centre of Dublin City University has made all of its resources, supports, and instructions freely available online. The Center is renowned throughout the world for its superior studies in bullying and internet safety. The mission of ABC is to work with a large network of academic and business collaborations to address the real-world issues of bullying and internet safety.

2. "BARNARDOS"

Barnardos is based in Dublin, Ireland and aims to provide services and collaborate with families, and communities to improve the lives of vulnerable children who had traumatic experiences as youngsters. The website offers assistance and provides services to families, young people, and children who are in need and have vulnerable backgrounds. The website has a section dedicated to "protecting and safeguarding children online" in which they provide workshops on internet safety and cyberbullying for children, young people, parents and teachers. These workshops are available in the school environment, in libraries, corporations or community centres.

3. "PDST"

The Professional Development Service for Teachers based in Dublin is the country's largest single support service offering professional learning opportunities to teachers and school leaders in a range of pedagogical, curricular and educational areas. They provide in particular useful resources, websites for Anti-Bullying Awareness Raising, Prevention and Intervention Strategies as well as Curricular Resources for Anti-Bullying for SPHE (Social, Personal and Health Education).

NATIONAL

1. **"BE SAFE ONLINE"**

Be Safe Online is a campaign of the Irish government that provides measures to keep the general population secure when using the internet. This website offers access to a variety of online safety tools, tips and resources for parents, guardians and teachers as well as children and young people. A range of online support services and materials are offered for several topics such as online bullying, sexting, online pornography, online gaming, personal data protection, mental health and online fraud. In addition, the website provides helplines with contact details as well as a hotline to report illegal content or cyberbullying.

2. **"WEBWISE"**

Webwise is the Irish Internet Safety Awareness Centre which provides information and free education resources regarding various internet safety issues and concerns. Moreover, it makes available a range of advice, videos and support for young people, teachers and parents. Besides, young people have the possibility to join the "webwise youth panel" which gives them the opportunity to raise their voice and share their opinion on subjects that matter to them, to be involved in the development of tools and programs for internet safety, to take part in international campaigns such as Safer Internet Day as well as join forces with other youth around Ireland.

3. **"TACKLE BULLYING"**

TackleBullying.ie is an Irish national website supported by the Department of Education and Skills (DES) under the 2013 Action Plan in Bullying (2013). The website aims to support teachers, parents, and young people in fighting bullying and cyberbullying by giving them tools in order to identify what they are, how they differ from one another and how to effectively prevent them from happening. The "Get Help" and Resources section offers parents, educators, and young people advice on what to do if they or someone else they know is being bullied, as well as some suggestions on how to be safe online.

5. International

1. "BETTER INTERNET FOR KIDS"

A new European strategy for a Better Internet for Kids (BIK+) was adopted by the European Commission in May 2022. Its goals are to enhance digital services that are age-appropriate and to guarantee that all children are respected, empowered, and protected online in accordance with the European Digital Principles. The BIK+ strategy is a kid-friendly version created to appeal and meet the needs of a younger audience by adapting the language, vocabulary, presentation and resources available. The Better Internet for Kids portal gives information, advice, and resources on better online concerns and provides hotlines and helplines as well as guidance for children and young people, parents and carers, teachers and educators.

2. GOOGLE FACT CHECK TOOLS

Google Fact Check tools encompass a set of initiatives and features developed by Google to combat misinformation and provide users with reliable information. These tools aim to promote fact-checking, enhance transparency, and support informed decision-making.

International News Outlets Fact Checking teams. Many news outlets have recognised the importance of fact-checking in today's media landscape and have established dedicated fact-checking teams. These teams play a crucial role in verifying claims, statements, and news articles to ensure the accuracy and reliability of the information being reported. Here are some notable news outlets with fact-checking teams:

- FactCheck.org
- Washington Post Fact Checking
- Politifact
- Reuters Fact Checking
- Snopes

3. THE NEWS LITERACY PROJECT

The News Literacy Project is a nonpartisan education nonprofit. The initiative is building a national movement to advance the practice of news literacy throughout American society. The organisation provides programs and resources for educators and the public to teach, learn and share the abilities needed to be smart, active consumers of news and information and equal and engaged participants in a democracy. creating better informed, more engaged and more empowered individuals.

4. SAFER INTERNET DAY

Safer Internet Day (SID) is the global day for online safety established and promoted by the European Commission, celebrated on the second Tuesday of February. The aim of the day is to encourage students to reflect on the conscious use of technological tools and the active role they can play in using the Internet in a safe and positive way. Among the initiatives of Safer Internet Day are conferences, prize competitions, and awareness-raising campaigns focused on topics related to cyberbullying, online child sexual abuse and exploitation, sexting, loss of privacy, gaming addiction and an excessively sedentary lifestyle or the risk of isolation, especially among younger users.

5. EUROPEAN SAFE ONLINE INITIATIVE

The main focus of the European SafeOnline Initiative is the improvement of media literacy levels among children and young people through the extensive media literacy education of their parents. Instead of attempting the development of a pilot experimentation project, the European SafeOnline project will scale up a recognised and proven innovation in the field of media literacy.

Associations and educational institutions in Belgium, Bulgaria, Cyprus, Greece and Romania contribute their own know-how to build a programme to educate parents and educators to become more aware of the opportunities and potential risks new media offer their children.

Conclusions

As part of the Erasmus+ project Strands, the partnership has conducted research all over Europe so as to gather resources, tips and advice on different aspects of keeping families and young people safe online.

Young people in Europe have access to a variety of opportunities thanks to the internet and other online technologies. Their use has become inevitable to perform a majority of activities in the framework of work, education, and entertainment. In order to protect young people and guarantee their safety without preventing them from accessing the digital world, a strong "partnership" needs to be created between parents

and schools to monitor the use of technologies and take joint action to prevent risks encountered online by youth.

Among the risks that have been selected and identified by the project consortium, it has been seen that the consequences for young people and their families can be heavy and leave mental, emotional and physical effects for life. Although the risks are different from each other such as loss of privacy, sexting, exploitation, cyberbullying etc, the aftermaths are the same. As a result, young people can suffer from a damaged reputation and thus have an increased level of anxiety, humiliation, which all lead to social exclusion, depression and in the worst cases suicide. Fortunately, families and schools can prevent those risks by successfully identifying the key signs that show that a kid is being victimised online. Most of the time, people tend to think that unusual or violent behaviour is caused by the "adolescent crisis" without looking further into the origin of the problem. It is thus crucial for all entities to not ignore those signs and remain attentive to young people's changes of behaviour. Moreover, all kinds of tips, advice and technical tools are available for young people themselves in order not to fall into traps online. That is why the more awareness and knowledge they have on the matter the more they can protect themselves while navigating the web.

Finally, **reporting is the key action to remember in the case of damage caused online.** The case studies gathered in this document show how important reporting is and how it can save someone's life. In order for young people to talk and report, **a relationship of trust** should be built between them, their families and their schools. Local, national and international support services as well as campaigns are also available for everyone to seek help and assistance.

In a nutshell, young people and families may be more vulnerable and exposed to risks when they are not aware of online dangers and how to protect themselves. That is why materials such as Strands E-Safety Manual are important in order to raise awareness about online threats without limiting access to online opportunities which are more than beneficial for students in today's context.

Resources

BENEFITS OF ONLINE OPPORTUNITIES AND IMPORTANCE OF SYNERGIES BETWEEN SCHOOLS AND FAMILIES

- Europe's digital future
- How do online platforms shape our lives?
- Opportunities and benefits online
- What are structure and agency?
- Being young in Europe today - digital world
- Synergy Between Schools and Homes
- Parental Involvement, Engagement and Partnership in their Children's Education

CYBER-BULLYING

- Cyberbullying: What is it and how to stop it
- Technological solutions for cyberbullying
- Cyberbullying: How to Identify, Resources to Help, and Innovative Solutions for the Future
- European Awareness Raising Campaign on Cyberbullying
- European AntiBullying Network
- Better Internet for Kids - Bulletin on cyberbullying
- Safer Internet Day: Commission campaign against cyber-bullying
- Everything You Need to Know About Cyberbullying
- From Cyberbullying to Well-Being
- Joining forces to Combat Cyberbullying in Schools

DANGEROUS ONLINE CHALLENGES

- How to respond to dangerous online challenges
- Most dangerous online challenges
- Tiktok Dangers
- Dangerous social media challenges
- Dangerous Internet Challenges
- What you need to know about hoaxes and online challenges

INTERNET ADDICTION

- Internet addiction: definition, assessment, epidemiology and clinical management
- Computer/Internet Addiction Symptoms, Causes and Effects
- Tips to Overcome Internet Addiction
- PsychoTherapyCyprus
- Cyprus Safer Day
- Cyprus Strategy for the online safety of kids
- The Systemic Institute of Cyprus: a Center for systemic applications, education, research and theoretical development.
- Cyberbullying: Text Neck Syndrome in Children and Adolescents

LOSS OF PRIVACY

- GDPR
- EU Commission - What is a Personal Data?
- EU Commission - Rights for citizens under GDPR FAQ
- Handbook on European data protection law by European Union Agency for Fundamental Rights
- Italian Garante Guides and handbooks for Children and Parents (in Italian)
- MIT - Facebook/Cambridge Analytica: Privacy lessons and a way forward
- Finalmente un po' di Privacy

WEB-TRACKING

- Avast: Web tracking: What it is and how it works
- Hotjar: Website tracking guide
- The electronic frontier foundation
- The best browsers for privacy
- The best ad-blockers
- What is VPN and how it works
- Zero-Cost Anti-Tracking Software & Extensions
- What is DNS and how it works
- Example DNS resolvers
- What is a password manager
- A list of password managers

FAKE-NEWS

- EUVSDISINFO
- New Initiative with Google
- BBC - How to talk to your kids about fake news
- UNICEF - Digital misinformation / disinformation and children
- Protecting children from fake news
- Social media advice hub
- Delaying or refusing COVID-19 vaccines: The effects of misinformation
- The effect of communication and disinformation during the COVID-19 pandemic
- EU Commission - Fighting disinformation

SEXTING

- Sexting within teenagers
- Sexting What It Is and How to Sext Safely
- Teens Social Media and Technology
- What is sexting and its consequences

Glossary

Bullying - an ongoing and deliberate misuse of power in relationships through repeated verbal, physical and/or social behaviour that intends to cause physical, social and/or psychological harm. It can involve an individual or a group misusing their power, or perceived power, over one or more people who feel unable to stop it from happening.

Cyberbullying - bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted.

Dangerous online challenges - an online challenge generally involves an individual recording themselves completing a challenge and distributing the video through social media channels.

School psychologists - uniquely qualified members of school teams that support students' ability to learn and teachers' ability to teach. They apply expertise in mental health, learning, and behaviour, to help children and youth succeed academically, socially, behaviorally, and emotionally.

Safety - the condition of being protected from or unlikely to cause danger, risk, or injury.

Security - the state of being free from danger or threat.

Social media - interactive technologies that facilitate the creation and sharing of information, ideas, interests, and other forms of expression through virtual communities and networks

Sexting - is the act of sending sexual text messages (the word is a combination of sex and texting). It often also involves sending nude or seminude photos and explicit videos of yourself.