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

CYBER STOP VIOLENCE

HANDBOOK

FOR YOUTH WORKERS, TRAINERS AND TEACHERS WORKING WITH YOUTH ON THE SUBJECT OF CYBER VIOLENCE

Instytut Nowych Technologii

CCS Digital Education

CSP innovazione nelle ICT

DIRECT Association

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

CYBER STOP VIOLENCE

September 2018

This handbook is available in 5 languages: English, Polish, Greek, Romanian and Italian and freely accessible on the project website : www.cyberviolence.eu

You can be updated on the project activity also following our Facebook pages, available in 5 languages.

The CyberViolence project 2016-03-PL01-KA205-035361 is implemented as part of the Erasmus+ program of the European Union (Action 2. Cooperation for innovation and exchange of good practices, Strategic Partnerships). The project implementation period is 24 months in April 2017 – March 2019.

Table of content

About the project 5
Module 1: Cyberviolence concept 8
Cyberbullying – a new form of bullying 8
Forms of cyberbullying 11
Antibullying Programme to stop violence 13
Recommendations: 15
Module 2: Cyberbullying and social media 17
The Social Media Landscape 17
Bullying vs Cyberbullying: a definition 20
The forms of cyberbullying 21
Slang useful to know 22
Module 3: Offline and online Identities, profiling and web tracking: 24
Keeping ourselves safe on the web 24
Identity 24
General aspects about offline Identity 24
Profiling 26
Web tracking 27
What is being collected through web tracking and why? 28
Location tracking 28
Recommendations 29
Recommendations for data privacy 29
Practical Advices 30
How to protect our online identity 30
How do they track us on the Internet 32
How to protect ourselves from web tracking 32
Best practices 33
Module 4: Working with youth 34
A brief description of youth as a social group. 34
Rules for working with young people 34
Internal motivation 35
Cooperative learning 36
Planning training for young people 36
Diagnosis 36
The initial part of the training 37
The right part of the training 38
End of training and evaluation 38
References 39

About the project

CyberViolence is a project aimed against violence on the Internet.

The Institute of New Technologies Association together with three European partners implements the international CyberViolence project as part of the Erasmus+ program.

The main problem about cyber violence is lack of knowledge and awareness about the problem of cyberbullying among young people, youth workers, teachers and parents. Among the youth, the problem is the lack of awareness of online threats, the lack of opportunities and the ability to respond to cyberbullying. Among the youth workers and teachers the problem is the lack of tools and methodologies for working with this topic, education and prevention. Among parents, there is no awareness of the problem and the ability to recognize the first signs of being a victim of cyberbullying. Among the target groups there are:

- **Youth** – the main target group of our activities. Young people are the most vulnerable to be a victim of cyberbullying due to the fact that they are vulnerable and inexperienced in social life;
- **Teachers, youth workers** – their role is to educate and prevent this negative phenomenon. They need new tools to know how to combat cyber violence among the students;
- **Parents** – when their child is a victim of cyberbullying they should be the first ones who are able to recognize the symptoms, but unfortunately they often lack the basic knowledge in this topic.

The project has a few main objectives, among which there are:

1. Improving the quality and relevance of education, through the development of new and innovative approaches (new scenarios for youth workshops, thematic comics, competitions, testing of these products, implementation and promotion of dissemination of results)
2. Developing a program to prevent cyberbullying, developing and providing a handbook and other resources for teachers;
3. Increasing knowledge about online threats, the consequences of online activities and the mental and emotional aspects of cyberbullying;
4. Introduction, development and promotion of innovative methods and tools in education by supporting schools and teachers interested in joining the program;

Promoting cross-border cooperation in education and prevention, as all project participants can learn from each other.

The project is implemented by 4 organizations from 4 countries and has a transnational character, as the Internet has no borders and cyberviolence is an international problem that has to be solved at the international level:

- Institute of New Technologies Association (Poland) – leader of the project
- Crystal Clear Soft (Greece) – partner,
- DIRECT Association (Romania) – partner,
- CSP – INNOVAZIONE NELLE ICT S.C.A.R.L. (Italy) – partner

About the handbook

This booklet is an important document for all dedicated youth workers and leaders, as well as interested NGOs, decision makers and citizens, who are familiar with the ways and goals of using pedagogical tools to stop cyber violence, promoting non-formal education and competences and skills which are in this case managing planning life goals and inclusion, empathy, the need to cooperate, acknowledging human rights, promoting differences and universal values of tolerance as-well as solving conflicts via communication and controlling conflicts. During the project, the participants will adopt new skills related to social dialogue and cooperation.

The number of training handbooks on non-formal learning focused on stop cyber violence is limited and insufficient. The lack of an adequate training framework (in formal education) for youth workers leads to inefficient use of the capacity of professionals working in the field. This handbook fills one of the gaps in the youth sector, namely the need for methodologies for the training of trainers capable of training youth workers.

The handbook modules that relate to the primary goal of the project are elaborated in a way that youth workers, trainers and teachers working with youth will acquire all the necessary knowledge and skills to prevent and stop cyber violence so the workshops can be utilized in further work for the wellbeing of their organizations, the local community and beyond.

We hope that this handbook will be used by youth workers and youth leaders to multiply the project message by using the methods and content of the Handbook. Following the priorities and aims of the Erasmus+ programme as well as their support project partners hope this handbook will serve as a useful tool on cyber violence prevention for active youth participation to find practical and sustainable solutions to stop the phenomenon of violence.

Module 1: Cyberviolence concept

This module gives an overview of the CyberViolence concept, types of bullying related to age, methods, channels of reaching, reactions, theoretical examples of cyberbullying situations that may affect young people with the described appropriate method of response.

There will be a schema of operation, to deal with difficult situations, solutions/remedies/responses, how to prevent, how to react, how to defend ourselves and others, support from the closest ones (family and friends) and the environment, social approach, media and public opinion and specific cases.

The project contributes to the raising the awareness of youth learning as an important tool for social inclusion. There needs to be more frequent and age-appropriate information for young people regarding their rights online and their responsibilities when using internet. We also recommend project toolkit of responses for trainers and educators and an educational approach to building empathy and responsibility online.

Learning by sharing experiences and work together to develop common quality criteria serve to all participating organizations to support the relevant procedures in their national systems.

Cyberbullying – a new form of bullying

Bullying is an international problem (see Smith et al., 1999).

Bullying ruins lives. It damages self-esteem, disempowers people and sews the seeds of prejudice. Last researches revealed that 1 in 2 people have experienced bullying in some form during their lives. This shocking statistic shows just how much more needs to be done.

In an academic context, there is a strong consensus in the research community that bullying is a form of social aggression (Björkqvist, Ekman, & Lagerspetz, 1982), which is characterized by three major criteria: intent to cause harm; repetition of the behavior over a period of time, and; an imbalance of power between the victims and the bullies (e.g., Olweus, 1993; O'Moore & Minton, 2004; Rigby, 2002). O'Moore and Minton (2004) extend this by arguing that just one particularly severe incident which contributes to an on-going sense of intimidation can constitute bullying.

In the European context bullying occurs in increasingly atrocious ways, such as: street fights, bombings, insults, harassment, cyberbullying. Dangerous, pathological behaviour like aggression and violence has gained new tools and, hence, adopted new forms. The phenomenon was diagnosed only several years ago and is nowadays referred to as "cyber-violence".

Cyber-violence is any online behavior that constitutes or leads to harm against the psychological, emotional, financial, and/or physical state of an individual or group.

Cyber-violence may be targeted at individuals or groups, the latter being more characteristic targets of cyber violence than of offline, physical violence, due to the ease with which a single perpetrator can gather information about and make contact with large numbers of people on the Internet. This is another aspect of online violence that can cause it to have widespread effects. *(European Network Addressing Cyber violence)*

Over the past 40 years, researchers have studied the phenomenon, which in 1970 was described as "**bullying**". Dan Olweus was one of the first researchers who made scientific studies of bullying. He defines bullying as follows:

We say that a student is being bullied when another student or a group of students;

- *say unkind or unpleasant things or make fun of someone or give any bad or hurtful nickname*
- *is ignoring or excluding someone from friends or deliberately fail to include some in various activities intentionally*
- *beating, kicking, shoving and bullies or threatens someone*
- *spread lies or false rumors about someone, sending nasty notes or trying to get other students to dislike someone*

The researchers Olweus, Smith, Ortega and Merchan agree on that in order to define a particular behavior as bullying, there must be at least three conditions applied: (i) an intent to harm the victim (ii) a repetition of the abusive behavior over a certain period (iii) an imbalance of power between the victim and the bully/bullies.

In the past, bullying may have been confined to school grounds; but with most young people now having access to smartphones, laptops and tablets, bullying and abuse can enter young people's homes and happen at any time, day or night. We heard harrowing accounts from children and young people who described cyberbullying as feeling 'inescapable', and in the most extreme of cases it has pushed young people to the verge of suicide.

Cyberbullying differs from traditional forms of bullying in a number of ways. For example Vande Bosch and Van Cleemput (2009) highlights that the power balance in cyber bullying is not dependent on the physical size, and may be based on higher technological skills or the ability to hide their identity

Bullying, once restricted to the school or neighbourhood, has now moved into the online world. Bullying through electronic means is referred to as "**cyberbullying**." The psychological and emotional outcomes of cyberbullying are similar to those of real-life bullying. The difference is, real-life bullying often ends when school ends. For cyberbullying, there is no escape.

In recent years the Internet and Information and Communication Technologies (ICT) have had an increasingly important impact on our everyday lives (Cross et al., 2009). Use is now thoroughly embedded in children's daily lives (Livingstone et al., 2011) and electronic communication is viewed by many children and adolescents as essential for their social interaction (Kowalski, Limber, & Agatston, 2008).

The connection between bullying and digital and social media created the phenomenon of cyberbullying, with new and unexpected effects of people. **Cyberbullying** is a form of repeated violence by one or more people towards other people defined victim through the use of the web, using computers or mobile devices.

Cyberbullying can hide the identity of a child who bullies so they aren't held responsible, even when the cyber bullying is discovered or reported to an adult. Due to the nature of electronic media, children can setup false accounts, or even make a parody account of the child that they are bullying. Anonymous cyber bullying is another one of the cyber bullying facts that results from the nature of electronic media, like the fact that cyber bullying can occur anywhere.

Technology also provides bullies the opportunity to harass the victim regardless of time and place. Therefore cyber bullying occurs outside of the physical limitations in the school environment or other

places where traditional bullying takes place. The bully or bullies no longer need to be located in the same place as the person or people they want to bother.

Cyberbullying has grown exponentially as a threat to online security over the last decade alone. To quote a few popular statistics, the 2017 Pew Research Center study on online harassment noted that around 40% of Americans have experienced online harassment personally, while around 62% of Americans already consider cyberbullying to be a major problem in our society. The study also stated that nearly one in five (18%) of individuals will experience more 'extreme' harassment such as physical threats, stalking, and online sexual harassment. Statistically, the harassment will target users over their political views, their physical appearance, race, gender, and sexual orientation respectively.

While the definitions of **cyberbullying** (Hutson, 2016), sometimes called **online bullying**, vary from source to source, most definitions consist of:

- *electronic forms of contact*
- *an aggressive act*
- *intent*
- *repetition*
- *harm* to the target

The technology, accessed through computers or cell phones, used to cyberbully includes:

- *personal websites*
- *blogs*
- *e-mail*
- *texting*
- *social networking sites*
- *chat rooms*
- *message boards*
- *instant messaging*
- *photographs*
- *video games* *(Feinberg & Robey, 2009)*

By definition, it occurs among young people. When an adult is involved, it may meet the definition of "cyber-harassment" or "cyber-stalking", a crime that can have legal consequences and involve jail time.

Cyberbullying occurs "*when someone repeatedly makes fun of another person online or repeatedly picks on another person through e-mail or text message or when someone posts something online about another person that they don't like*" (Cyberbullying Research Center, 2016).

Cyberbullying is as an aggressive, intentional act distributed by an individual or group, using contact in an electronic medium, continuously and relentlessly against someone who cannot stand up for himself or herself easily (Smith et al., 2008).

We developed this definition because it is simple, concise, and reasonably comprehensive and it captures the most important elements. These elements include the following:

- ***Willful:*** The behavior has to be deliberate, not accidental.
- ***Repeated:*** Bullying reflects a pattern of behavior, not just one isolated incident.
- ***Harm:*** The target must perceive that harm was inflicted.

- ***Computers, cell phones, and other electronic devices:*** this, of course, is what differentiates cyberbullying from traditional bullying

According to the European Commission, cyberbullying is repeated verbal or psychological harassment carried out by an individual or group against others. It can take many forms: mockery, insults, threats, rumours, gossip, "happy slapping", disagreeable comments or slander. Interactive online services (e-mail, chat rooms, instant messaging) and mobile phones have given bullies new opportunities and ways in which they can abuse their victims.

Violence in cyberbullying occurs through messages, films, and photographs, intimidating writings through social media or published on websites. Examples of cyber-violence include (but are not limited to) malicious text messages or emails, rumors sent by email or posted on social networking sites, sharing of another's intimate pictures/videos/texts without consent, online bullying, harassment, cyberstalking, blackmail, expressions of racism, homophobia and misogyny.

Vandebosch, Van Cleemput, Mortelmans, and Walrave (2006) argue that it is not essential that aggression be repeated on the part of the bully in order for it to constitute cyberbullying. For instance, content created or shared just once by the cyberbully can remain online over time, and therefore can be viewed or shared by those who witness the content. In such an instance, the repetition is characterized by the number of witnesses as opposed to the number of actions on the part of the cyberbully.

Additionally, the power imbalance in cyberspace is somewhat less clear than in the real world. Although in cases of traditional bullying, power can take the form of physical size, in the cyber world power may be constituted by the capacity to hide one's identity (Vandebosch et al., 2006). It is somewhat more difficult to remain anonymous in instances of traditional bullying.

There are several actors involved in cyberbullying:

- Bully/bullies
- Victim
- Observers

It's important to understand that the role of the bully and the victim are interrelated and sometime the role can be change, if we change the point of view: sometime the victim can become a bully or a persecutor.

Rey and Ortega (2007) divide traditional bullying into five main forms:

1. *physical*
2. *verbal*
3. *gestures*
4. *exclusion*
5. *blackmailing*

All types of bullying are linked to a real risk of causing psychological harm, impaired performance in education and lack of social achievements.

Forms of cyberbullying

One way to understand cyberbullying is to classify it according to media or form:

- By the media where the assault is going on, such as text messages, picture messages, phone calls, e-mail, instant messaging or web pages.

- In line with the assault`s character, such as flaming arguments, harassment, slander, pretending to be others, disclosure of private information, exclusion, persecution and defamation.

These classifications will change as the technological development changes. The following overview gives a closer insight in different types of cyber bullying:

1. ***By type of media*** (from Smith, 2006)

•SMS: Sending or receiving abusive text messages via mobile phone.

•MMS, Snapchat, etc: Take, send or receive unpleasant pictures and/or video clips using mobile phones.

•Phone calls: Make or receive disturbing phone calls, such as evil nonsense phone calls, or anonymous calls.

•Malicious or threatening e-mails sent directly to a victim or emails with malicious content about a victim sent to others.

•Threats or abuse when participating in Chat: chat rooms, for example during online gaming.

•Harassing instant Messages Messaging: (IM), for example on Facebook, Skype

2. ***By the type of behavior*** (Willard, 2007)

•**Flaming:** an intense, brief discussion which often includes harassing, rude and vulgar language, insults and sometimes threats. "Flaming" can occur via text messages or instant messengers, in blogs, on social networking sites, in chat rooms, on message boards or via online computer games

•**Harassment:** repeated distribution of nasty, mean and insulting messages.

•**Slander:** send or publish gossip and rumors about a victim in order to damage his or her reputation or friendships.

•**False identity:** pretend to be someone else and sending or publishing materials to create problems for the person who owns the profile. Aiming to damage his or her reputation or friendships.

•**Outing:** disclosure of secrets or personal and private information in order to humiliate. A common method is to forward a message from the victim containing intimate or personal information.

•**Rip:** persuade someone to reveal secrets or humiliating information, then share this online

•**Exclusion:** deliberately and viciously exclusion of someone from a group or online forums. For the victim, exclusion from participating in online activities with peers can cause a feeling of rejection.

•**Cyber stalking:** persecution, repeated intense harassment and slander, which include threats and creates significant fear.

•**Harassment:** use of Internet or mobile phone for verbal or visual attacks. Predators can post comments in blogs or sending text messages from a mobile. They can also take pictures of the victim or steal a picture from a source on the Internet and then change the image in a humiliating way or add harassing comments and publish them online so others can see. A special trend ("happy slapping") involves filming of people being beaten up, and then upload the video online.

•**Posing:** a form of indirect attack where a bully publishes content on the Internet in the name of the victim. This may take place if a bully knows the victim's username and password, and can log on and access the victim's online accounts. When the bully pretends to be the

victim, he or she may say bad things to or about the victim's friends. This can get the friends or peers to reject the victim, as they think it was the victim who said it.

Antibullying Programme to stop violence

Professor Mc Guckin et al. (2012) believe that children and young people with a positive self-image, and who learns to act with assertiveness, often have a better understanding of how they should behave in difficult situations.

Specialist within psychology Solfrid Raknes (Norway, 2013) developed some tips for how parents can make the child more robust and enhance their self-image:

- Help your child to identify his/her own feelings
- Teach your child to talk positively, encouraging and supportive for themselves in difficult situations.
- Talk about nice things that happened during the day.
- Facilitate good relationships and positive experiences with adult caregivers. This makes it easier for children to go to adults for help when they need it.
- Facilitate for your child to develop friendships, and let them bring their friends home. Friendships make your child better equipped to cope with adversity.
- Encourage independence and give the child tasks it can handle.
- Teach your child that adversity is something we can use to become stronger. Life is not just easy, and you do not always get what you deserve.
- You cannot prevent your child from facing tough experiences, but you can influence how your child can handle them.

Children do not always tell their parents about cyberbullying that takes place among friends and peers. Parents should listen attentively when their children talk about their online experiences, and acquaint themselves with the various arenas of digital communication that young people are using (such as *Facebook, Instagram, snapchat,* etc.). If the child has told about a bullying episode, a parent's first response may be to confirm that the child made a good choice: - *Thank you for telling me this.*

If online content is upsetting and inappropriate, and the person or people responsible are known, parents need to ensure they understand why the material is unacceptable or offensive and request they remove it.

If the person responsible has not been identified, or refuses to take down the material parents should contact the social networking site directly to make a report and request the content is taken down. The material posted may be in breach of the service provider's terms and conditions of use and can therefore be removed. Some service providers will not accept complaints lodged by a third party.

In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly. Before parents contact a web service provider, it is important to be clear about where the content is, for example by taking a screen shot of the material that includes the web address.

Parents should stay calm when a child tells them about an incident where they were bullied online. A calm and balanced response helps to keep the lines of communication open with your child.

Kowalski (2008) also suggests that the parents and their child should agree on which cases where the child's parents inform the parents of the counterparty about negative content and/or contact online.

By providing children positive feedback, parents can influence behavior without discouraging the child. Well-intentioned, but negatively charged words from adults can be perceived in ways that were not indented.

Self-esteem comes from feeling loved, secure (Taylor, 2011). Parents can increase their child's resilience against negative consequences of bullying by building up a positive self-esteem. They can promote their child's confidence by developing, emphasizing and acknowledge the child's strengths.

The following are some things that parents may wish to consider teaching their children about using the Internet safely (source - https://www.gov.uk/)

- Make sure you use the privacy settings.
- Always respect others – be careful what you say online.
- Be careful what pictures or videos you upload. Once a picture is shared online it cannot be taken back.
- Only add people you know and trust to friends/followers lists online. When talking to strangers, keep your personal information safe and location hidden.
- Treat your password like your toothbrush – keep it to yourself and change it regularly.
- Block the bully – learn how to block or report someone who is behaving badly. • Do not retaliate or reply to offending e-mails, text messages or online conversations.
- Save the evidence. Always keep a copy of offending e-mails, text messages or a screen grab of online conversations and pass to a parent, a care giver or a teacher.
- Make sure you tell an adult you trust, for example, a parent, a care giver, a teacher, or the anti-bullying coordinator or call a helpline.
- Most social media services and other sites have a button you can click on to report bullying. Doing this can prevent a bully from targeting you and others in the future. Many services take bullying seriously and will either warn the individual or eliminate his or her account.
- While you are on your mobile phone make, sure you also pay attention to your surroundings.

Parents can contact the school, leaders in the youth environment if bullying occurs within an organized activity, police or other agencies if they are considering this as relevant according to the seriousness of what has taken place.

What parents can do if their child has been cyber bullied:	**What parents can do if their child is involved in bullying others:**
• Listen attentively to your child • Remain calm • Block the cyber bully • Do not reply • Secure evidence • Find out what is wrong • Make it clear that it is the bully who has a problem, not the victim • Create an atmosphere of security • Strengthen your child's self-esteem • Report the problem	• Develop an accurate and objective overview of what the ongoing cyberbullying involves. • Find out underlying reasons for this behavior. • Consider outlining rules for the child in order to promote responsible use of Internet and mobile in general. • Consider measures to follow up on your child's use of Internet and mobile phone in an appropriate manner. • Promote and develop the child's capacity for empathy and respect for others. • Build your child's confidence and self-esteem. • Facilitate energetic children "catharsis", let them unleash energy and frustration in a constructive way.

Although cyberbullying usually starts at school, and very often involves peers, cyberbullying incidents may occur outside school boundaries. It is very important that schools invest in raising students' knowledge and awareness about the characteristics of new media, about features such as their digital footprint (Chadwick, 2014).

The Schools Anti-Bullying Programme contain four main components:

1. A network of professionals who are trained to implement the anti-bullying programme in participating schools;
2. Resources for teachers and in-service training provided by the trainers;
3. Resources and information for parents and other members of the community provided by trainers;
4. Trainers taking a consultancy role for the duration of the programme in the participating schools.

Besides parents, school should inform all relevant actors that can contribute to solve the situation, such as psychological counsellors and electronic service providers.

Building a supportive school environment, raising awareness of the problem, providing training for teachers, students, parents, and other school staff, incorporating cyber bullying into the curriculum, publicize antibullying measures, and assuring the indispensable monitoring and evaluation are among the several practices that shape a wholeschool approach, and thus contribute to the prevention of bullying behaviours.

Through antibullying campaigns, several good elements and approaches will be identified that may shape a well-organized, concrete and coherent policy outline that could be used in developing a common EU anti-bullying policy or in developing each country's national anti-bullying policy.

In terms of developing a school anti-bullying policy, it is recommended that the following elements are included:

- A positive school ethos with a focus on respecting the individual;
- Awareness raising that bullying is considered to be an unacceptable behaviour among school management, teachers, pupils, and parents/guardians; implementation of supervision and monitoring to counter bullying across all areas of school activity with assistance from students;
- Design of procedures for noting and reporting bully/victim problems as an integral part of the school Code of Behaviour and Discipline;
- Provision of support for victims, bullies, and peers, including counselling;
- Inclusion of local agencies in combating bullying as a form of anti-social behaviour as it is desirable to involve the extended school community beyond the school grounds;
- Ongoing review and evaluation of the effectiveness of school anti-bullying policy to assess the prevalence and types of bullying within the school.

One of the important measures to limit risky behavior is to enable children and young people to develop digital skills. In order to be able to guide young users; parents and professionals need to develop their own level of competence.

Recommendations:

- Social media platforms must be age-appropriate, and companies should pilot approaches to identify under-13s and gain explicit parental consent.

- Social media companies should enable children and young people to understand their rights and responsibilities, including their behavior towards others.
- Social media companies should provide timely, effective and consistent responses to online bullying.
- The Government should put children's experiences at the heart of internet safety policy development.
- Educators and parents should teach children and young people how to be safe and responsible online, and ensure they know how to respond positively to online harms such as cyberbullying.

There is a vital need for a collaborative effort from society, schools, teachers, parents, and young people to determine policy and practice, and it is of particular importance that young people feel that their voices are heard in these matters which affect them:

- Cyberbullying must be included in a whole school community approach to bullying, which empowers students to report victimization to seek help either for themselves or their peers;
- Education regarding staying safe in cyberspace, responding effectively when faced with aggression, and improving online social skills are necessary for young people;
- Both parents and teachers must take responsibility in dealing with abusive behavior in cyberspace and must offer support for those victimized;
- It is important that teachers receive training both in pre-service and professional development training with regard to group dynamics and conflict management;

Module 2: Cyberbullying and social media

This chapter aims to provide a guidance on the phenomenon of cyberbullying in social media.

It follows the process shown in the following figure.

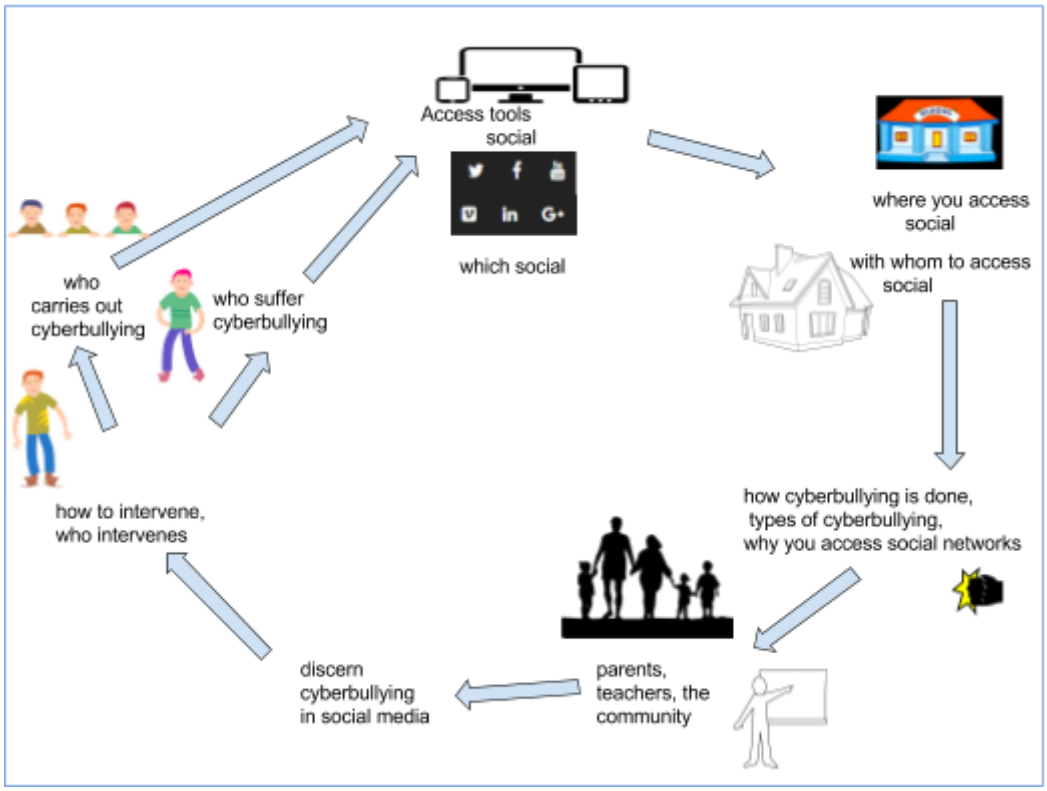

Figure 1 Cyberbullying the social media process

The phenomena cyberbullying on social media is described and analyzed in the following, considering:

- definition of social media and cyberbullying vs bullying
- actors involved in cyberbullying in social media (the bully, the victim, the observers/spectators)
- identification of the context in which cyberbullying phenomena occur (at school, at home, in groups, with friends)
- analysis of how cyberbullying and types of cyberbullying are done
- analysis to recognize cyberbullying: parents and teachers
- analysis to counteract the phenomenon and understand how to intervene on the bully, on the victim and on those who witness the phenomena of cyberbullying, laws, regulation of social media (Twitter, Facebook,...) at international level.

The Social Media Landscape

Social media is a generic term that refers to technologies and practices on the web allowing people to interact, share text, photos, images, video and audio content.

Professor Andreas Kaplan and Michael Haenlein[1] defined social media as a group of web applications based on the ideological and technological assumptions of Web 2.0, which allow the creation and exchange of user-generated content.

Social media brought a dramatic change in the way people learn, read and share information and contents. Using sociology and technology Social Media transformed the monologue (from one to many) in dialogue (from many to many) and the users/consumers in producers, we talk about "prosumers"[2].

They become very popular because they allow people to use the web to establish personal or business relationships. Social media are also referred to as user-generated content (UGC) or consumer-generated media (CGM).

The use of Social Media is very popular and the numbers of people using these channels are really impressive but there are some differences in terms of age and gender.

Table 1 Some Facts about Social Media[3]

Facebook is the largest social media network in the world and has members from almost every generation, but some demographics are more attracted to it than others.	• Facebook has 2.01 billion unique monthly visitors • Facebook users are 53% female and 47% male • 75% of Facebook users spend 20+ minutes on Facebook every day • 83% of women who use social media use Facebook, versus 75% of men who use social media • 63% of seniors aged 50-64 who use the internet are on Facebook, as well as 56% of online seniors over 65
YouTube is the second largest social media network in the world, and it also has the power of Google behind it.	• YouTube has 1.3 billion unique visitors per month • YouTube users are 38% female and 62% male • YouTube reaches more 18-34 and 35-49-year-olds than any cable network in the US • 80% of YouTube users are outside the US
Instagram isn't nearly as big as YouTube, but it is the fastest growing social media network, and that growth shows no signs of stopping anytime soon.	• Instagram has 700 million unique visitors per month • 80% of Instagram users come from outside the US • 59% of internet users between 18 and 29 are on Instagram, along with 33% of Internet users between 30 and 49 • 17% of teens say Instagram is the most important social media site (up from 12% in 2012)

[1] https://en.wikipedia.org/wiki/Social_media
[2] https://en.wikipedia.org/wiki/Prosumer
[3] The data are from: How to Find Social Media Audience for Your Business: From Demographics, All the Way to Which Platforms to Use and What to Post https://revive.social/find-social-media-audience/

Twitter has 328 million unique visitors per month. It's a channel that can't be ignored for business.	• 37% of Twitter users are 18-29; 25% are 30-49 • 69 million Twitter users are based in the United States • 79% of Twitter users are based outside the United States
Snapchat is currently the second fastest growing social network. It's the most suitable channels for teenagers	• over 300 million active users on Snapchat every month • 173 million people use Snapchat every day • 71% of Snapchat users are under 31 years old • 45% of Snapchat users are 18-24 years old
Pinterest it's a fast-growing social with around 150 millions of users, it's the best choice for visual communications, great for business connected with a photo.	• 81% of Pinterest users are women • 40% of new signups are men; 69% are women • The median age of a Pinterest user is 40, but most active users are under 40 • 60% of Pinterest users are from the US
Linkedin it's the social for professional connections rather than for social activities.	• 40 million college students and recent graduates are on LinkedIn • 70% of LinkedIn users are from outside the US • 44% of LinkedIn users make more than $75,000 per year • An average user spends 17 minutes monthly on LinkedIn

In the following pictures, you can see some trends in the use of social media.

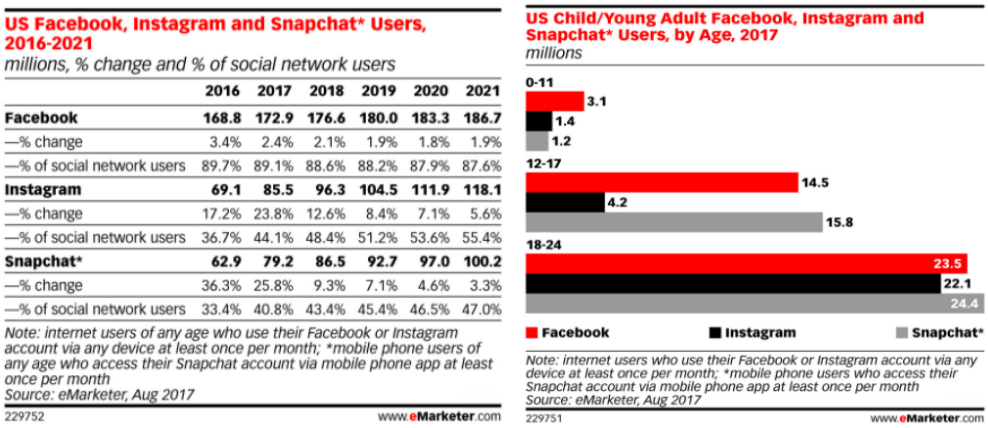

Figure 2 Facebook, Instagram, and Snapchat users – source: TechCrunch

Bullying vs Cyberbullying: a definition

Cyberbullying is a form of violence by one or more people towards other people defined the **victim** through the use of the web, using computers or mobile devices.

This violence occurs through messages, films, photographs, intimidating writings through social media or published on websites.

Bullying and cyberbullying mainly involve young people, but adults are also involved in this form of violence.

The table below shows the comparison between cyberbullying and bullying in a document of the Ministry of Education of the Italian University of Research[4].

Table 2 Differences between bullying and cyberbullying

Bullying	Cyberbullying
Only students in the class and/or the school are involved;	Children and adults from all over the world can be involved;
Usually, only those who have a strong character, capable of imposing their own power, can become a bully;	Anyone, even those who are victims in real life, can become cyberbullying;
Bullies are students, classmates or Institute companions, known to the victim;	Cyberbullies can be anonymous and solicit the participation of other anonymous so-called "friends" so that the person does not really know who they are interacting;
Bullying actions are told to other students in the school where they took place, are limited to a specific environment;	The material used for cyberbullying actions can be spread worldwide;
Bullying takes place during school hours or on the journey from school to school, school to home;	Aggressive communications can take place 24 hours a day;
School or class group dynamics limit aggressive actions;	Cyberbullies have ample freedom to do online what they couldn't do in real life;
Need for the bully to dominate in interpersonal relationships through direct contact with the victim;	Perception of invisibility on the part of cyberbullies through actions hidden behind technology;

[4] http://www.miur.gov.it/bullismo-e-cyberbullismo

Visible reactions from the victim and visible in the act of bullying;	The absence of visible reactions from the victim which do not allow cyberbullies to see the effects of his actions;
The tendency to evade responsibility by taking violence on a playful level.	Personality splitting: the consequences of your actions are attributed to the created "user profile".

The forms of cyberbullying

Cyberbullying can appear in various forms, such as for example in gaming cyberbullying, which is often called "griefing". Different types of cyberbullying are described in the following table.

Table 3 Different types of cyberbullying

Flaming	Sending violent and vulgar messages.
Harassment or Stalking	Sending repeated messages to an individual.
Denigration	Dissemination of false news.
Identity theft / unauthorized access and Impersonation Masquerading	Identity theft. Masquerading is a situation where a bully creates a fake identity to harass someone anonymously. In addition to creating a fake identity, the bully can impersonate someone else to send malicious messages to the victim
Tricky Outing	It consists of having the trust of the victim and then spreading his or her confidence.
Ostracising/Exclusion	Intentional exclusion of a person from a group.
Happy slapping	Dissemination of online material in which the victim is resumed while suffering violence.
Trolling	Attacking a person on important personal or family matters.
Roasting	Attacking a person until he or she bends, no longer resists attacks.
Creating Websites, Blogs, Polls and More	Development of vilification websites, vilification blogs, vilification surveys.

Self-cyberbullying or digital self-harm	As the case of Hannah Smit[5] sending messages denigrating on the web.

Slang useful to know

The use of slang and jargon is very common among teens and it helps in creating a sense of community. It could be useful to know the language used by teens[6] and especially some acronyms that can be monitored. In the following table, you can find some examples, but of course, these things are different in any community and can change very rapidly.

PHRASES TO BE AWARE OF

GNOC: Get naked on camera

FBOI: A guy who's just looking for sex

WTTP: Want to trade pictures

FINSTA: Fake Instagram account

PAL: Parents are listening

1174: Meet at a party

FAM	Refers to someone who is a close friend
LIT/TURNT/TURNT UP	Something that's active or popular, can also refer to being stoned or drunk
SMH	"Shaking my head", meaning "I don't believe it" or "that's so dumb"
KMS/KYS	"kill myself", "kill yourself"
DABBING	Reference to concentrated doses of cannabis; also a dance craze
SNATCHED	On point, very good, or well styled
NETFLIX AND CHILL	Getting together and hooking up
AF	Short for "as f**k", used to mean "extremely"
BASIC	Used to refer to someone viewed as a boring or conforming person
💯	Emoji used to mean pride or general acceptance of an idea
🍆	Emoji used to refer to the penis
🍑	Emoji used to refer to the butt
🦋	Emoji used to mean "ejaculate", often used in conjunction with the tongue emoji
MOS	Mom over shoulder
9 AND CD9	Parents are nearby
99	Parents are gone
WTTP	"Want to trade pictures?"

Figure 3 Some acronyms used by teens

5 https://www.bustle.com/p/what-is-self-cyberbullying-a-dangerous-new-trend-involves-teens-sending-bullying-messages-to-themselves-3072212

6 Do you know what GNOC and PAL mean? Experts reveal the dangerous teenage sexting slang all parents should know "(ref: http://www.dailymail.co.uk/sciencetech/article-4596096/The-dangerous-teenage-texting-slang-parents-know.html#ixzz50NZj6t8j

A child can be involved in cyberbullying in different ways. A child may be bullied or present in a situation of bullying. Parents, teachers and other adults may not be aware of all social media platforms and apps used by a child. More digital platforms a child uses, more opportunities there are to be exposed to potential cyberbullying.

Many of the warning signs that cyberbullying is happening around a child's use of the device. Because children spend a lot of time on their devices: computers, tablets and especially mobile phones, increases or decreases in use may be less noticeable. It is important to pay attention when a child shows sudden changes in digital and social behavior.

Teachers, school administrators, parents, and trainers are in unique positions to use their skills and roles to create safe environments with positive social norms. They are also in positions where they may notice changes in youngsters' behavior in group settings, such as when a group of children focuses attention on a child. There are things you can do in class or other group settings to deal with or prevent cyberbullying[7].

[7] https://www.stopbullying.gov/cyberbullying/tips-for-teachers/index.html)

Module 3: Offline and online Identities, profiling and web tracking:

Keeping ourselves safe on the web

In the early 1990s, Internet users used to feel shielded behind an electronic veil of anonymity, able to take on any persona they pleased. The internet has changed hugely in the last 20 years, in ways that directly affect our online identity and privacy. Online services of all kinds today have adopted technologies that build profiles of customers, offer product recommendations, and keep personal histories that can be long-lived and extremely detailed. Data sharing between these web-based businesses also affects our online identity and privacy. Through data sharing, a service provider can link subsets of personal data to a mass of data we may have thought was confined to another persona or context.

While some Internet users appreciate the convenience those digital identities afford, others worry about how much of their personal information is being stored and how this information is being shared.

Identity

This section will help explain the various different identities and profiles that represent people online and offline both from a social science and a technical perspective. Children and young people may use the internet for a host of different reasons. One of them is to express, and potentially experiment with their identity (Turkle, 1995, 1996, 2011). Using social network sites such as Facebook, online role playing games such as World of Warcraft, and social media such as Twitter, they can connect with others, interact with them, share ideas, images and movie clips, and engagein a variety of versions of 'digital flea picking'. Developing, expressing and experimenting with identities is a central element of growing from childhood into maturity, and therefore it is worthwhile to investigate how the internet affords and inhibits young people's abilities to engage in online self-exploration.

The data presented here is based on the work presented in the Primelife EU project book[8], Roger Clarke's publications[9] and Goffman's perspective on identity (Goffman, 1959), which remains very influential to this day.

General aspects about offline Identity

As individuals interact with other individuals and organisations in many different relations, all of which are connected to different roles of the individual, Goffman (1959) defines identity as **"the result of publicly validated performances, the sum of all roles played by the individual, rather than some innate quality**". In this respect, all different roles or characteristics can be seen as **partial identities.**

From a practical perspective, **our identity** is **the sum of our characteristics**, including our birthplace and birthday, the schools we attended, our shoe size, our language, ethnicity, religion, gender, social class, sex, generation and so on. Some of those characteristics never change, such as our birthday, and some change over time, such as our age or hair colour. In simple words our identity is that we are who we are and what we do.

[8] Camenisch, J., S. Fischer-Hübner & K. Rannenberg (2011). *Privacy and Identity Management for Life*. Springer Science & Business Media.

[9] http://www.rogerclarke.com/DV/DigPersona.html#Prof

Different (kinds of) relationships involve different kinds of information constituting the **individual's identity.** A single individual therefore consists of different characterizations linked to the different contexts in which he/she operates.

According to Goffman (1959) different contexts impose different rules on behaviour and people play different roles (as in a theatre play) in different contexts. Also they present different faces of themselves. Thus, we may say that individuals give different performances in everyday life.

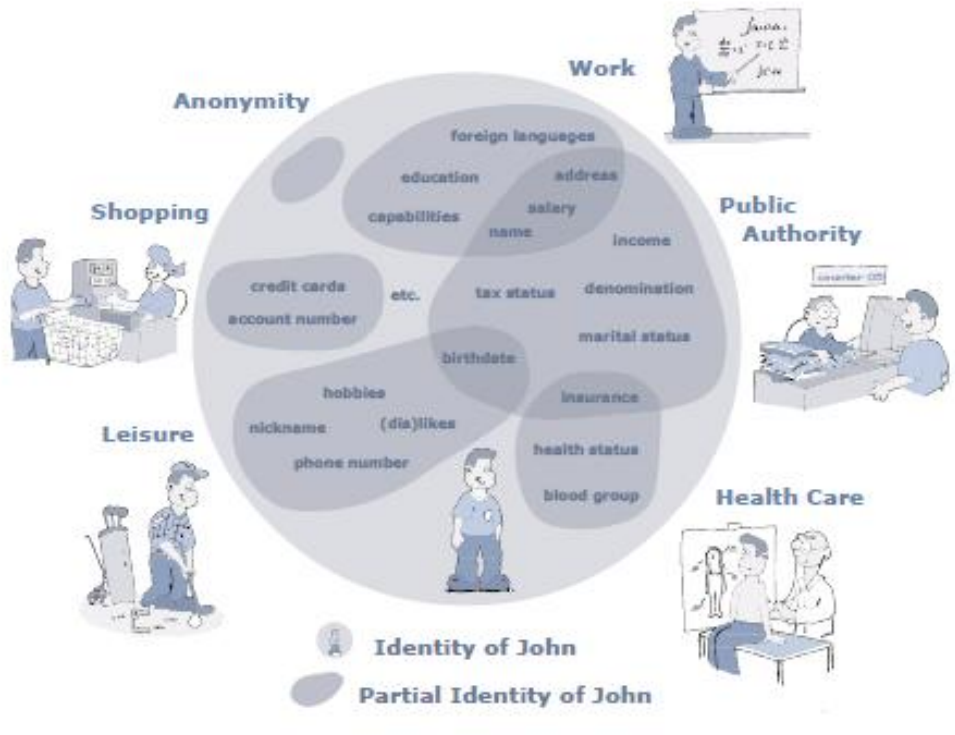

Figure 4 An identity comprised of multiple different identities [source: Primelife project D1.3.1].

Online identity is valued

Our identity has value, as does each of our online partial identities. Our identity is valuable not only to us but to others as well:

1. It is of value to the individual, because his identity reflects him and gives him access to the resources they desire.
2. Second, it is of value to the service provider who relies on our assertion of identity, for example the bank or a social networking site, such as Facebook. They are the holders of the resources we want. Our identity is a business asset to those entities.
3. Lastly, our identity is of value to the thieves and other illegitimate users of our identity who want it to access resources they are not entitled to. As the value of our partial identities grows, the information becomes more attractive to thieves.

Identity theft, broadly, is the loss of control over one or more of our partial identities.

As any online partial identities may contain private data, it is important to manage and protect them appropriately.

Profiling

Profiling refers to the use of "sophisticated pattern recognition", the above mentioned identifiers, by governments and businesses, which employ this technique to distil meaningful information from massive amounts of data about individuals or groups of people, for example for the purpose of targeted advertising and personalized services in the case of businesses, or policing, crime prevention and detection, combating terrorism and surveillance in the case of governments. Profiling revolves around the idea that large sets of randomly collected data about individuals and groups of people can generate interesting, surprising and meaningful correlations that machines, with their vast powers of calculation can detect, while we as humans cannot.

As the name suggests, profiling may lead to the creation of extensive *profiles*, in which information about individuals or groups of individuals are accumulated, stored, and used for the purposes cited above.

The risks of profiling

Many of the risks the Internet poses can be mitigated if, especially, youth more proactively preserve their privacy online. Doing so requires them to be more aware of the consequences of disclosing identifying information, and of guidelines for determining when it is appropriate to do so. Unfortunately, many young people do not easily recognize situations in which disclosing information might put them at risk.

Given the complexity of the data itself, combined with the complexity of human behavior patterns, one of the concerns relating to profiling is the occurrence of 'false positives' (Rubinstein *et al.*, 2008): the software finds correlations in the data that are deemed meaningful, when in fact the correlation is accidental and random.

Moreover, one of the most serious concerns surrounding profiling is the *opaqueness* that surrounds it. It is often unclear to internet users when, where and for which purposes they are profiled. It is also unclear to users in which cases they are presented with decisions that build on profiling processes, or even *that* this may be the case.

These profiles may thus be used to target individuals – both grown-ups and children! – with

commercial offers, without these individuals knowing that this is the case, or which profiles or digital traces these recommendations are based on. Especially in relation to children, this is a serious issue.

Many online games for children, for example, abound with subtle (or not so subtle) product recommendations made on the basis of children's actions within the game or even outside, for instance when they've linked their profile in the game to their profile on social media platforms such as Facebook. Since such recommendations may be personalized, based on profiling, the seduction to buy the products offered may be much greater for these children. This may draw children, sometimes from very early ages onwards, into commercialized worlds in which the goal is to sell as many products as possible, while the children themselves are oblivious to this fact.

Web tracking

In this section we will explain what web tracking is and get better insight on its types**. Web tracking** is the activity (and ability) of a website (using special software tools) to keep tabs on website visitors.

There are many ways that companies may use to track browsing behaviour on websites. These include:

Cookies: These are small bits of text that are downloaded to our browser as we surf the web. Their purpose is to carry bits of useful information about our interaction with the website that sets them. Contrary to a common belief, cookies do not contain software programs, so cannot install anything on a computer. Cookies generally do not contain any information that would identify a person. Usually they contain a string of text or "unique identifier". This acts like a label. When a website sees the string of text it set in a cookie, it knows the browser is one it has seen before.The cookies that appear to cause the most controversy are for managing the advertising we see on a website. This cookie can record when and where we saw an advert, where in the world we might have been when it happened and whether we clicked on it. The cookie will send this information to the cookie owner, who records this data and uses it to make sure we don't see the same advert too many times.

Flash cookies: also known at "locally shared objects". These are pieces of information that Adobe Flash might store on our computer. This is designed to save data such as video volume preferences or, perhaps, our scores in an online game.

Server logs: when we load a page on a website, we are making a request to that website's server. This server will log the type of request that was made and will store information such as: IP address (which will allow website owners to infer location), the date and time the browser loaded the page, what page was loaded, and what site or page the browser was on before it came to that page (referrer). Server logs form the basis for web analytics and can only be seen by the owners of the website.

Web beacons: these are small objects embedded into a web page, but are not visible. They can also be known as "tags", "tracking bugs", "pixel trackers" or "pixel gifs". This is very useful to companies that want to learn if readers are opening their the emails they send. When the web beacon loads, companies can tell who opened the email and when. Often advertisers will embed web beacons in their adverts to get an idea of how often an advert is appearing.

What is being collected through web tracking and why?

Trackers collect information about which websites we're visiting, as well as information about our devices.

One tracker might be there to give the website owner insight into her website traffic, but the rest belong to companies whose primary goal is to build up a profile of who we are: how old we are, where we live, what we read, and what we're interested in. This information can then be packaged and sold to others: advertisers, other companies, or governments.

The companies tracking we are unrelated to the website we're visiting. Called "data brokers", they tend to have stock-market sounding names like DoubleClick, ComScore, and cXense (though DoubleClick is actually owned by Google). Their entire business is built on the selling of "customer data".

They are also joined by more well-known companies. Some of these are even visible: Google's red G+ button, for example, is a tracker; Facebook's "like" thumb is a tracker; and Twitter's little blue bird is also a tracker.

Location tracking

Location tracking gives a very detailed picture of who we are, where we go and who we spend time with. See how our location is tracked through our phone, our wifi connections, the websites we visit, and the social media platforms and email providers we use.
Our devices - computers, mobile phones, and tablets - are constantly telling others where we are. **Our mobile phone** in particular is a very effective tracking device: Where we go and it records our location all the time - even when we're not connected to the internet.

Location information collected over time can tell a surprisingly **full story** about who we are and what our life looks like. Add publicly-available addresses, tweets, photos, and/or our phone records, and the story gets really detailed.

Location data can also be used to map out our relationships with others. If we and another person, or other people, are in the same place at specific times of the day, it's possible to infer what relationships we have with these people - if, for example, they are co-workers, lovers, roommates, or family members. This kind of detailed picture can be valuable to all kinds of people and organisations. For one, it can be sold by companies to make money; it can also can be used to predict where we'll be at a given point in the future.

If we have location information on our phone turned on for pictures, this information will get embedded in the picture (i.e. the picture's metadata will include where we took the picture). When we send or upload these pictures we can share our location data without thinking about it. Most social media providers extract location data when we upload the picture, but there are still many ways in which location data can be aggregated from the pictures we share.

Recommendations

Recommendations for data privacy

EU data protection rules, also known as the EU General Data Protection Regulation (or GDPR), describe different situations where a company or an organisation is allowed to collect or reuse your personal information[10]:

1. When is data processing allowed?

A company or an organization is allowed to collect or reuse your personal information:

- When they have a contract with you – for example, a contract to supply goods or services (i.e. when you buy something online), or an employee contract
- When they are complying with a legal obligation – for example, when processing your data is a legal requirement, for example when your employer gives information on your monthly salary to the social security authority, so that you have social security cover
- When data processing is in your vital interests – for example, when this might protect your life
- When you are to complete a public task – mostly relating to the tasks of public administrations such as schools, hospitals, and municipalities
- When there are legitimate interests – for example, if your bank uses your personal data to check whether you'd be eligible for a savings account with a higher interest rate.

2. Agreeing to data processing – consent

When a company or organisation asks for your consent, you have to make a clear action agreeing to this, for example by signing a consent form or selecting yes from a clear yes/no option on a webpage.

It is not enough to simply opt out, for example by checking a box saying you don't want to receive marketing emails. You have to opt in and agree to your personal data being stored and/or re-used for this purpose.

You should also be given the following information before you decide to opt in:

- information about the company/ organisation that will process your data, including their contact details, and the contact details of the Data Protection Officer (DPO) if there is one
- the reason why the company /organisation will use your personal data
- how long they intend to keep your personal data
- details of any other company or organisation that will receive your personal data
- information on your data protection rights (access, correction, deletion, complaint, withdrawal of consent)

All this information should be presented **in a clear and understandable way.**

3. Specific rules for children

If your children want to use online services, such as social media, downloading music or games, they will often need approval from you, as their parent or legal guardian, as these services use the child's

[10] https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm

personal data. Your child will no longer need parental consent once they're aged over 16 (in some EU countries this age limit might be as low as 13). Controls to check parental consent have to be effective, for example by using a verification message sent to a parent's email address. See module 1 for specific legislation in the partners' countries.

4. **Access to your personal data**

You can request access to the personal data a company or organisation has about you, and you have the right to get a copy of your data, free of charge, in an accessible format. They should reply to you within 1 month and have to give you a copy of your personal data and any relevant information about how the data has been used, or is being used.

5. **Deleting your personal data (the right to be forgotten)**

If your personal data is no longer needed or is being used unlawfully then you can ask for your data to be erased. This is known as "the right to be forgotten".

These rules also apply to search engines, such as Google, as they're also considered to be data controllers. You can ask for links to web pages including your name to be removed from search engine results, if the information is inaccurate, inadequate, irrelevant or excessive.

If a company has made your personal data available online and you ask for them to be deleted, the company also has to inform any other websites where they've been shared that you've asked for your data and links to them to be deleted.

To protect other rights, such as freedom of expression, some data may not be automatically deleted. For example, controversial statements made by people in the public eye, might not be deleted if public interest is best served by keeping them online.

Practical Advices

How to protect our online identity

Although we are not able to control everything that is known about us online, there are steps that we can take to better understand our online identities and be empowered to share what we want, when we want. This section aims to help us to better manage our online identity[11].

These are some practical advices helping us to avoid divulging sensitive personal information to individuals or entities that plan to exploit it.

1. **Add plug-ins to web browser:** Plug-ins have the ability to check websites and alert us to ones that are known to be malicious.
2. **Protect password**.
   - ❖ **If a password is easy to guess**, then it is easy to steal. **Select passwords that you can easily remember, but that they aren't easy for other people to guess.** Be especially careful to choose different, hard-to-guess passwords for each of the websites that are especially important to us, such as online financial services.
   - ❖ **Avoid using the same password** for multiple websites, so if one website is compromised,

[11] More information on the issue can be found at the Internet Society tutorials: https://www.internetsociety.org/tutorials/manage-our-identity/

our stolen credentials can't be used at other sites. If we want to select passwords that are related to make them easy to remember, try customizing the password for each site by adding a few characters (such as the site name). This won't fool a dedicated attacker but it will keep out anyone who tries our password on other websites. The key principle here is to keep things practical while protecting against the most likely attacks.

- ✓ **Use two-factor authentication**: If our bank or other important service providers offer this, unless our bank agrees to take all the liability in case our password is compromised. Password resets are meant to help us when we've lost a password (or have been locked out). Every website has a slightly different technique for resetting a password. Here are the most common steps that are followed for resetting passwords.
- ✓ **When resetting our password**, we are asked to answering some personal "security" questions we have previously answered. We may receive an email with a link that enables the reset or a new password might simply be emailed to us. For websites that use security questions to validate our identity, use factual information (which makes it easy to remember) in ways that are difficult to guess. For example, if the question asks for the name of the first school we attended or the name of the first street we lived on, answer with the second school we attended or the second street we lived on. That way, even someone who knows a lot about us will have trouble answering the questions. Also, remember that we don't have to give "logical" answers, as long as they make sense to us and are memorable to us. For instance, if the security question asks "What is our favorite color", there is nothing to stop us giving "three", or "Monica's eyes" as the answer and it will be a lot harder for an attacker to guess.

3. **Email protection**: Here are some tips we can adopt to help protect our email, which helps protect our online identity.
   - ❖ **Select email addresses wisely**
   - ❖ **Select different email addresses** for each of our multiple online personas: When we have multiple online personae, such as professional, personal, and academic, select a different email address for each. Carefully choosing the right persona when someone asks for our email address can prevent problems later on. For example, our work or school email may not be very private if the company or institution claims the right to read or archive email on their servers.
   - ❖ **Use 2-factor authentication** wherever available. It combines different authentication techniques to make it more difficult for an attacker to compromise the whole authentication process. For instance, it may combine "something we know" (like a password) and "something we have" (such as a phone - which also means the authentication process can make use of two separate communication methods). This kind of 2-factor authentication would work as follows: we first enter our password. A second code is then sent to our phone. Only after we enter it we get access to our account. To subvert the authentication process, an attacker now has to not only know our password, but also be able to intercept a separate message, in real time, sent to our phone.

The Online Trust Alliance website at https://otalliance.org/ has a resource list to help us learn more about the technologies that can help protect our identity on the Internet.

How do they track us on the Internet

To see ourselves who is tracking us we can use:

- Lightbeam: Lightbeam is an add-on for Firefox that shows we which third parties are present when we visit a website. If we then go to a new website, Lightbeam will show we not just which third parties are active on that site, but which third parties have seen we on both sites; and so on as we visit more websites.

We can install it through Firefox's main menu, or go to Lightbeam --> **add to Firefox** To start it up, click on the Lightbeam icon at the top of our browser → browse the internet for a while → check the visualisation.

- Trackography (Tactical tech project): News websites are a great source of information about us. What newspaper we read, and which articles, can say a lot about our political views, general interests and even things like our sexuality or religious affiliations. Trackography allows us to see who is tracking we when we read the news online - among other things, like which countries our data travels through along the way.

  Go to Trackography → *select our country* → *select the media we read* --> see how many companies are reading over our shoulder. If we click on a specific company, we can also find out more about their privacy policy.

How to protect ourselves from web tracking

To take more control over our data, we can take the following steps:

Change settings for boosting our privacy as we browse the internet and use social media

- **Firefox:** https://myshadow.org/how-to-increase-our-privacy-on-firefox
- **Chrome:** https://myshadow.org/how-to-increase-our-privacy-on-chrome
- **Twitter:** https://myshadow.org/how-to-increase-our-privacy-on-twitter

Install add-ons/extensions to block trackers

There are some very effective bits of software we can install to block trackers, encrypt our website connections, or stop spying ads from running - all of which can make a big difference to our privacy. It is often a good idea to use more than one tool to address the same privacy concerns.

Each tool uses a different technique to block trackers, and some might affect our browsing experience. The best approach is to just try them out, and find the mix that works for us.

- **Privacy Badger:** Install Privacy Badger from website (Firefox, Chrome)
- **Adblock Plus:** Install AdBlock Plus from website (Firefox, Chrome, Opera, IE, Safari, and others)
- **Disconnect:** Install from the Disconnect website
- **HTTPS Everywhere:** Install HTTPS Everywhere from website (Firefox, Chrome, Opera)
- **NoScript:** Install NoScript from website (Firefox)

Best practices

- **SAFER INTERNET CENTRES** have developed various educational resources aimed at helping teachers, parents and carers, and children and young people, to discover the online word safely. Now you can access all of these resources in just one place via this resource gallery.

- **SAFER INTERNET DAY RESOURCES**: Safer Internet Day (SID) 2018 took place on Tuesday, 6 February 2018 with a theme of "Create, connect and share respect: A better internet starts with you". You can find a gallery of resources - from across the Insafe network of Safer Internet Centres and beyond - to help you celebrate SID in your school... and indeed promote a safer and better internet all year through! Search by keyword or language to find resources to meet your needs, or just browse the list here.

Module 4: Working with youth

"Be yourself – find your own way. Get to know yourself before you want to get to know children. Realize what you are capable of (…). You are the only child you have to meet, educate and educate first of all"

Such an advice was given to the educators by the outstanding Polish teacher Janusz Korczak. It applies to children's educators, but you can also refer it to educators, educators, and youth teachers. Knowing yourself, working on your own weaknesses and developing your strengths, and above all, authenticity in contact with the mentees will allow for effective work with young people.
Youth work differs from working with children or with adults. It is connected with constant confrontation with teenage rebellion, with strong emotions, but also with the great absorption of young minds. If a youth worker manages to gain the trust of young people and encourage them to work together, he can do a lot for himself, for his pupils and entire communities.

A brief description of youth as a social group.

To talk about teaching young people, we need to think about who we mean when we say young people. Researchers do not agree on the definition of youth and youthlness, or even an age that could be a determinant to qualify a given person in the category of youth. As a rule, the category of adolescents includes persons aged from 11 to 21, although the upper limit is often moved even to 30 years of age. However, the biological criterion of age is not enough to define young people.
Researchers dealing with youth issues emphasize the transient nature of this period of life. It serves the adoption of certain life roles and the acquisition of skills to implement them. At the same time, it is a very turbulent time when an individual is struggling with biological maturation and the search for identity. This is associated with confusion and anxiety. Young people eagerly focus on groups around the idea or doctrine, are prone to indoctrination and testing of different ideologies. Among adults, they also look for guides and reject the authorities. The period of youth is the time of internal and external conflicts. Attempts to define yourself and the world around you. Young people build their worldview, determine what standards and values they want to be guided in their lives. They become independent from the family and acquire social skills. Despite many common features, young people are a heterogeneous category. Differences arise from the social and cultural context in which young people are embedded and from individual characteristics.

Rules for working with young people.

A number of difficulties can be encountered in working with youth, including resistance to involvement, lack of trust. These difficulties can be countered by applying several principles:

- Listen to the voice of young people, treat them as equal partners.
- Include young people in all stages of joint work - from planning, through implementation, to evaluation.
- Use a language that everyone can understand.
- Organize meetings in places of friendly and well-known young people, eg in cultural centers.
- Create an atmosphere of mutual respect and friendship, and above all, make sure that everyone feels safe.

Young people are much more willing to engage in activities that arouse their curiosity, relate to their interests, encourage physical activity, are rich in various external stimuli such as colorful presentations, illustrations, paintings, scents, sounds / music. It is also important to clearly define the purpose for which young people would be involved. This goal must be consistent with the needs and values of the participants, otherwise the group will not want to take action.

Internal motivation

Work with young people should be based on arousing internal motivation, which is a force that drives people to take action despite the lack of external rewards. We talk about internal motivation when we do something, because it makes us happy, gives us a sense of satisfaction and allows us to develop in an area that is important to us. The activity undertaken is a reward in itself. This type of motivation favors engagement and creativity, which is why it is worth developing in young people.
Factors that increase internal motivation:

- **Curiosity** - young people are more eager to learn what is interesting for them.
- **Sense of influence** - young people are more willing to get involved if they have the opportunity to choose and have a real influence on what is happening to them.
- **Recognition** - wisely used praise has the effect of strengthening internal motivation, but it too often has the opposite effect.
- **Cooperation** - young people willingly cooperate with each other, inspire each other and encourage them to act.
- **Competition** - the desire to compare your results with the results of others may be a source of internal motivation. However, if the discrepancies between the results are very large, the motivation drops.
- **Challenges** - clearly defining the goal and the ability to track the level of its implementation favors the development of internal motivation. The goal should be achievable, but requiring effort, and above all should be consistent with the values and aspirations of a given person.
- **Pleasure** - if any activity gives us pleasure, we not only take it more willingly, but also remember more about it.

The most important element of learning young people is experiencing. Young people should, if possible, use their own: knowledge and skills to learn about the unknown and gain new habits. However, if the existing knowledge and skills are insufficient, the teacher or trainer acts as an expert and gives the knowledge already tested. Students, however, should have the opportunity to test it in a practical task.

Cooperative learning

Learning based on group cooperation supports learning in an atmosphere of mutual respect and friendship, thanks to which it is an effective method. Nevertheless, it is worth combining workshop participants into groups in a thoughtful way. It should be remembered that better results, both in the development of individual members and for the whole group, bring work in a more diverse group. Optimally, groups should consist of four people, so that during a given task can go to work in pairs, after a while, return to the discussion with the whole group. If the specificity of the task allows it, it is worth asking the participants to assign roles (eg a person making notes, a person responsible for materials, a watchman, etc.) so that no one remains passive. Exercises can also be divided into phases and asking individual students to guide their implementation (eg stage I - discussion and brainstorming, stage II - translation of the discussed issues into objectives and activities, stage III - presentation of results).

Planning training for young people

Diagnosis

A very important element of planning work with young people is recognizing her training needs. If we do not get to know them, we will not know if the program, tools and techniques that we plan will be appropriate and effective.

In order to create a good diagnosis of the needs of the young people's environment, partners should be involved, for example: schools, local institutions, local governments, as well as the young people themselves. By looking at the needs of young people from different perspectives, we will have a better chance of accurately recognizing the real problems.

It is not enough to ask what training and wants young people want. You have to be inquisitive, do not stop at one question, but explore the topic and look for the hidden causes of the existing state. The "5 Why" method can be used for this purpose. The first element of this method is to gather as much information about a given problem as possible. Examples of questions we can look for answers:

- What is the situation? What's happening?
- Since when does it look like this? Has something changed? Has it ever been different?
- What is the scale of the problem? How many people are he concerned?
- What will be the consequences if nothing changes?

Then determine who can help us look for the cause of the problem. You can use the brainstorming method for this purpose. Once you know what the problem looks like and who to ask about its causes, you can proceed to the appropriate stage of the "5 Why" method, that is, to ask "why?". To know the real cause of the problem, the "why" question should be asked on average 5 times, e.g.

Problem: Youth do not participate in activities of local cultural institutions.

1. Why do young people not participate in activities of local cultural institutions?
   Because they do not want to.
2. Why are young people not willing to participate in activities of local cultural institutions?
   Because they prefer to spend time at home in front of a computer.
3. Why do teenagers prefer to spend time in front of the computer?

Because they are afraid of building relationships in the real world.

4. Why are teenagers afraid of building relationships in the real world?

Because they evaluate they social skills low.

5. Why do young people assess their social skills low?

Because they rarely have the opportunity to train these skills.

In the above case, the solution may be to involve the youth in activities that will allow the development of interpersonal skills, initially in small groups.

An important principle in diagnosing needs is to avoid simple categorization. In the above case, the division between active and inactive youth comes first, but maybe inactive youths in some areas are willing to take the initiative and guilty. After asking more questions, such a division can be misleading.

When diagnosing the needs of young people, it is worth using attractive and interesting diagnostic methods that will require the participation of the subjects, not just their answers to the questions. Such methods can be walking, mapping, field game, workshops. Attractively diagnosed may be an incentive for young people to participate in classes later.

The diagnosis should be completed with a report that should be brief, comprehensible to everyone, attractive and available to those interested.

The initial part of the training

Once I was diagnosed and needed to carry out the same needs and thoroughly update them. It is necessary to formulate the goals of these activities. Young people are more willing to get involved, get to know each other. When planning an action, one should approach the diagnosed needs as well as the possibilities and barriers of implementation from the age, place of residence, and interest saved. On this basis, determine their classes, their time and place, and then plan the class collection.

Classes or classes should begin with getting to know each other and building an atmosphere of trust and kindness. This can be served by integration games and so-called icebreakers. These are games that allow participants and youth worker to learn something about themselves, overcome shyness and encourage cooperation. In the initial part of the training, it is also worth determining the purpose of the classes and their structure.

An important element of the course is to define the rules that all participants and leaders will follow. It can be served by a contract agreed and signed by everyone. It helps to avoid various embarrassing situations in the training room. Because young people like to decide for themselves and influence what is happening around them, it is better to abandon the authoritarian imposition of principles that will be respected and set them together. The teacher can encourage participants to submit policy proposals, ask orientation questions, or organize discussions. The rules set out in the contract, all participants should agree, and in order to prove it, it is worth signing. Written contract should be hung in a visible place and it should remain until the end of training or a training cycle. In problem situations, the trainer can refer to established rules. If during the training it turns out that the contract ran out of some rule, with the consent of the whole group, you can add it. Also, if any of the saved rules prove to be difficult to comply with and all participants will want to plot it - it is possible. The contract can be updated at every stage of the training - provided that all these changes are accepted.

The right part of the training

Once the participants and the trainer are familiar with each other, the aim of the course is clear to everyone, what topics will be discussed and when there are breaks and everyone accepts the training contract, you can proceed to the right part of the course.

When arranging a class schedule, one should bear in mind how young people learn and provide them with a variety of stimuli and activities.

WE REMEMBER

10%	• what we read
20%	• what we hear
30%	• what we see
50%	• of what we hear and see at the same time
70%	• what we say
90%	• what we say and do

The individual modules of the classes are clearly separated from each other. People remember better what is at the beginning and the end - the most important issues should be found in these places. The lecturers should, therefore, do many "beginnings" and "ends" through appropriately planned breaks and summaries of individual batches of materials.

It's a good idea to introduce traffic to the right part of the training, because the activity improves the brain's functioning. If you use the lecture method, it is worth making small spacers every 8-10 minutes. It can be a question for participants, a joke or a short exercise.

End of training and evaluation

Each training or other form of classes should have its ending and summary. It serves to organize the transmitted knowledge. At the end of each class it is worth gathering the participants' opinions on their satisfaction with the completed training. However, do not stop at subjective assessments, because they say nothing about whether the goals of the training have been achieved. Therefore, it is necessary to consider other forms of evaluation. The easiest way is to test the knowledge, but probably no teenager likes tests. A better solution is to check whether participants are able to use the acquired knowledge in a practical task. You can also conduct individual and group interviews or invite participants of the educational process to participate in the summing-up workshops. Applications from the evaluation should be presented in the form of a written report.

References

American Library Association. (2002). The Children's Internet Protection Act. http://www.ala.org/cipa/

Bell, Vicki and Denise de la Rue. n.d, Gender harassment on the Internet. http://www.gsu.edu/~lawppw/lawand.papers/harass.html

Belsey. (2006). Cyberbullying: An emerging threat to the "always on" generation. Available at http://www.cyberbullying.ca

Biegel, Stuart. (1996). Constitutional issues in cyberspace: Focus on 'community standards'. *Los Angeles Daily Journal*, February 22, http://www.gseis.ucla.edu/iclp/feb96.html

Cyber-stalking.net. (2002). Statistics. http://www.cyber-stalking.net/statistics.htm

Dixon, S., Craven, E., Hayley, C., Weber, S. (2017). Preventing and eliminating cyberviolence initiative: Needs assessment findings. Atwater Library and Computer Centre. Montreal, QC. Retrieved July 13,

Egan, Jennifer. (2000) Out in cyberspace. *The New York Times Magazine*, December 10, 2000.

Finkelhor, David,Kimberly Mitchell, and Janis Wolak. (2000). Online victimization: A report on the nation's youth. http://www.missingkids.com/download/nc62.pdf

Herring, Susan C. 2001. Gender and power in online communication. *Center for Social Informatics Working Papers*. http://www.slis.indiana.edu/csi/WP/WP01-05B.html

Kiesler, Sara, Jane Siegel and Timothy W. McGuire. (1984). Social psychological aspects of computer-mediated communication.*American Psychologist* 39: 1123-1134.

Magid, Lawrence. (2000). When kids surf, think safety first. *San Jose Mercury News*, June 17.

McRae, Shannon. (1996). Coming apart at the seams: Sex, text and the virtual body. In L. Cherny and E.R. Weise (eds.), *Wired_women*, 242-263. Seattle: Seal Press.

Mc Guckin C, Cummins PK, Lewis CA. (2010). Cyberbullying among children in Northern Ireland: Data from the Kids Life and Times surveys. Psychology, Society, & Education.

Mc Guckin, C. (2013). School bullying amongst school pupils in Northern Ireland: How many are involved, what are the health effects, and what are the issues for school management?

Office for Internet Safety (2008) A Guide to Internet Safety for Children. Available at http://www.internetsafety.ie/website/ois/oisweb.nsf/page/286BBF5D3E55C002802 574C10036C6CB

Office for Internet Safety (2012) Get With It – A guide to cyberbullying. Understanding and identifying cyberbullying to help protect your children. Available at http://www.internetsafety.ie/website/ois/oisweb.nsf/page/7C7F45450A4CDC2B8 0257514004B6B10/$file/GWIT_Cyberbullying_Dec12.pdf

Olweus, D. (1993). Oxford: Blackwell.

Olweus, D. (1999). Sweden, i P.K. Smith mfl. (red.) The nature of school bullying. A cross-national perspective. Routledge: London.

O' Moore, M. (2010). Dublin: Veritas. Understanding school bullying. A guide for parents and teachers

O'Moore, M. og Kirkham, C. (2001). Self-esteem and its relationship to bullying behaviour, Aggressive Behavior

O'Moore & P. Stevens (Eds.), Bullying in Irish education: Perspectives in research and practice. Cork, Ireland

O'Moore, M. (2012). Cyber-bullying: the situation in Ireland. Pastoral Care in Education.

Pfaffenberger, Brian. (1997). "If I want it its OK": Usenet and the (outer) limits of free speech. *The Information Society* 12.

Purdy, N. & Mc Guckin, C. (2011). Disablist bullying: An investigation of student teachers' knowledge and confidence. Armagh, Northern Ireland: The Standing Conference on Teacher Education North and South (SCoTENS).

Shim, Young Hee. 2002. Remarks at UNESCO Chair Symposium on Women's Rights, Cyber Rights. Seoul, South Korea, May 31, 2002.

Smith PK, Morita Y, Junger-Tas J, Olweus D, Catalano R, Slee P. (Eds.) (1999). The nature of school bullying: A cross national perspective. London and New York: Routledge.

Smith PK, Pepler DJ, Rigby K. (Eds.) (2004). Bullying in schools: How successful can interventions be? Cambridge: Cambridge University Press.

Smith, P. K. & Steffgen, G. (Eds.) (2013). Cyberbullying, technology and coping. Oxfordshire: Psychology Press.

Spertus, Ellen. (1996). Social and technical means for fighting on-line harassment. http://www.mit.edu/people/ellens/Gender/glc

Thomas, Karen. (2002). Girls know way around Net, parents.*USA Today*, February 13, 2002.

Tokunaga, R.S. (2010). Following you home from school. A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behaviour.

Vandebosch, H. og Van Cleemput, K. (2009). Cyberbullying among youngsters. Profiles of bullies and victims.

Vandebosch, H., Van Cleemput, K., Mortelmans, D., & Walrave, M. (2006). Cyberpesten bij jongeren in Vlaanderen. [Cyberbullying amongst youngsters in Flanders]. Brussels: viWTA.

WHO@ (Working to Halt Online Abuse). (2002). http://www.haltabuse.org/

Appendix: Resources on the Web

- WHO@ (Working to Halt Online Abuse) -http://www.haltabuse.org/
- EU Kids Online, 2013: www.eukidsonline.net
- WiredPatrol (formerly CyberAngels) - http://www.wiredpatrol.org/
- CyberTipline -http://www.cybertipline.com/
- SafetyEd International - http://www.safetyed.org/
- http://cyberviolence.atwaterlibrary.ca/wp-content/uploads/2016/08/Atwater-LibraryPreventing-and-Eliminating-Cyberviolence-Initiative-press-draft.pdf