#DigitSafe

Boosting digital safe spaces and resilience

Digital Resilience Handbook

Contents

Introduction

The #DigitSafe, Boosting Digital Safe Spaces and Resilience Project, aims at empowering young people to become resilient and safe digital citizens, enabling them to address some of the challenges and negative impacts of the digital era. This is in line with Goal 6, "Information & Constructive Dialogue", of the EU Youth Strategy 2019-2027.

The #DigitSafe project pursues fostering a wider and deeper knowledge amongst young people on the two key topics of Cybersecurity & Hate Speech, and Security & Privacy. The project particularly aims to reach the most vulnerable groups of young people, through building safer digital common spaces and practices whilst boosting their capacities in terms of digital resilience.

This project also wants to achieve the following three specific main objectives:

1. To promote digital citizenship among young people in participating countries by, in accordance with the EU Youth Strategy 2019-2027, empowering them with practical and compiled information about Security & Privacy, and Hate Speech & Cyberbullying.

#DigitSafe

2. To provide young people, especially the ones with fewer opportunities who often lack information and data literacy, with the necessary competences to enhance their digital resilience.

3. To develop an innovative methodology that translates the compiled relevant information of this handbook into a multichannel public awareness campaign, utilizing the most common audiovisual communication practices, language, tools, and trends amongst young people. This will be a multimedia and multichannel strategy exploiting the vast number of content creation possibilities accessible to every user in the current social media landscape, aimed at strengthening the ability of the youth to make rational choices, and know their digital rights.

This Digital Resilience Handbook will offer comprehensive and unified guidance, covering practical information and tips (including legal, psychological, training, and open-learning resources), and make key recommendations to help youth acquire a more in-depth knowledge of their rights,

digital risks and threats in the context of these topics. It will raise awareness of the opportunities and resources available to build skills for dealing with issues arising from young people's current digital lives. It will empower youth to become engaged digital citizens and foster a safer digital world. It will curate a vast amount of information, unifying it in a more useful and comprehensive way.

#DigitSafe

Boosting digital safe spaces and resilience

1. Cyberbullying

1.1. What is cyberbullying?

At the European level, multiple definitions of cyberbullying have been found, incorporating various aspects depending on the specific characteristics of the countries in which the study has been carried out (Belgium, Bulgaria, The Netherlands, and Spain). However, the study developed in 2016 by the Policy Department of Citizen's Rights and Constitutional Affairs belonging to the European Parliament "Cyberbullying Among Young People," has produced a fairly accurate and homogeneous definition that can be used transnationally in the European Union:

....

- Cyberbullying describes those situations in which bullying is taking place on the internet mostly through mobile phones and social media. Cyberbullying corresponds, thus, to an equally aggressive and intentional act, carried out through the use of information and communications technologies (ICTs)."

....

As with offline bullying, cyberbullying usually involves the following three key participants:

#DigitSafe

- The **perpetrator**: *the person carrying out the aggression.*
- The **victim***: the person who suffers the aggression.*
- The **bystanders**: *those who see what is happening between the bully and the victim, but they are not directly involved in the bullying.*

The conduct must occur intentionally and repeatedly and there must be an imbalance in the power relations between the aggressor and the victim.

There are key features of Cyberbullying which facilitates its identification and comprehension:

- <u>Cyberbullying is malicious and never accidental</u>. The cyberbully has the clear and conscious goal to harm the victim, to cause pain, humiliate him/her/them, to make him/her/them suffer physically or mentally.

- <u>It is performed from a position of power</u>. The cyberbully always has an advantage and he/she/them holds a position of superiority. Depending on the environment in which cyberbullying is taking place, it could mean committing cyberbullying with a group against one victim who is alone.

Aggressors can take advantage of a non-aggressive or vulnerable victim, unable to defend himself/herself/themselves.

- It is repetitive, aimed at <u>intimidating, angering, or embarrassing</u> the victims. An isolated aggressive action is not cyberbullying yet. It becomes cyberbullying when the aggression is repeated over and over again against the same person (or the same people).

Digitalization has multiplied the channels through which bullying can be perpetrated via the internet. However, some of the most common ways in which cyberbullying victims are attacked are as follows:

Social networks

Mobile phones

Messaging platforms

Gaming platforms

#DigitSafe

In order to clarify which illegal actions would fall under cyberbullying, here are some examples:

- *Spreading lies or posting embarrassing photos/videos of someone on social media.*
- *Sending offensive messages or threats through messaging platforms.*
- *Sending malicious messages under someone else's identity.*

1.2 The importance of cyberbullying and its consequences: raising awareness and how identify it

Identifying Cyberbullying

One keyway in which to tackle cyberbullying is being able to identify it and look out for the warning signs. There is no universally agreed definition of cyberbullying internationally or on a European level.

However, the European Commission defines cyberbullying as "repeated verbal or psychological harassment carried out by an individual or a group against others through online services and mobile phones."(2) According to the Council of Europe, cyberbullying is distinctive from other types of bullying

(2)'Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.8.

#DigitSafe

due to the risk of public exposure, the complex roles of observers, and the size of the audience that comes with digital technologies and communication.(3)

To create a more tolerant and safer world online, cyberbullying must be tackled on a wider scale at both an individual and organizational level.

The consequences of Cyberbullying cannot be taken lightly or regarded as mere jokes, as it not only denies the emotions and suffering of the victim but also normalizes this type of violence in the digital environment. Cyberbullying's consequences can be long-lasting and can affect the victims in many ways.

We could highlight as the main consequences of Cyberbullying:

- **Mental and emotional consequences** Victims may feel sad, ashamed, embarrassed, stupid, depressed, angry and anxious. Victims usually lose their interest in the things they used to love. They develop a lower self-esteem, or they feel isolated, incapable of communicating with their peers. Sometimes victims of cyberbullying can become "victims-aggressors", replicating the behavior and bullying others.(4)

(3) https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)
(4) Joint Research Centre (2013). Social Networks and Cyberbullying among Teenagers

#DigitSafe

- **Physical consequences** The stress and anxiety that a victim suffers can lead to physical problems such as feeling tired because of sleeping disturbances or experiencing real health symptoms such as stomach aches or headaches.
- **Legal consequences** The feeling that they are being ridiculed or bullied by others often prevents the victims of cyberbullying from reporting or trying to deal with the problem. This, together with the slow evolution in the legal classification of the crime, means that it often goes unpunished, and it encourages the repetition of attacks.

Raising awareness of cyberbullying to prevent it is essential. The first step in identifying cyberbullying is to have a clear definition of what it involves. In Europe, policy decisions have been taken and numerous programs have been defined and implemented to prevent cyberbullying.

The Cyberbullying Research Centre has developed a series of structured tips on how to proceed in order to prevent cyberbullying and secure ourselves as users. Prevention is always the best option to fight against this problem.

Addressed to young people:

- Stay up to date with privacy settings - Social Media sites and programmes are modifying and updating their privacy settings frequently. Make sure that you are familiar with the new profile options and keep as much information as possible restricted to those you really trust.

- Restrict access to your contact information - Do not give out your email or phone number to people that you do not know. Also, keep your email and phone number off social media sites.

- Learn internet etiquette - To prevent potential problems with other internet users, learn social conventions related to interaction in cyberspace.

- Don't send inappropriate pictures or videos - Remember that today's boyfriend, girlfriend or partner can be tomorrow's scorned lover. You do not want someone with inappropriate pictures or videos of you posting them online and sharing them with the rest of the world. Don't put yourself in the position of having to worry about this.

#DigitSafe

- Google yourself - You should always know what is being said about you. It is often surprising to find information you thought was private show up in public databases, new articles or on social media pages that have been indexed by search engines.

- Do not accept friend requests from strangers - If you do not know the person who is sending you a friend or follower request, ignore it. Most social media sites and apps also give you the option to block the user if you like.

- Use site-based controls - Disable search options on certain social media sites to prevent anyone in the general public from searching for you or messaging you.

- Keep your information protected - If using a public computer or wireless, be sure to log off any site you are on when you walk away from that computer – even for a minute.

- Be skeptical in online interactions - Even among people you trust, it is risky to reveal too much information because you never know for sure if the person you think you are communicating with is really there, or if they are alone.

- Guard against people - Remember that some people have a lot of time on their hands and all they want to do is make life miserable for others. Don't let them. Resist putting too much personal or private information online that could be used to harass or humiliate you and resist interacting with them in any way.

Addressed to teachers and parents:

It is important for organizations, schools, workplaces and individuals to commit themselves to tackling cyberbullying because of the impact that cyberbullying can have on victims. The research developed by the Cyberbullying Research Centre in 2021 "Cyberbullying: Identification, Prevention and Response" gave an extensive explanation of how teachers and parents could address cyberbullying in terms of identification and prevention.

Educating the community about a responsible use of devices focused on digital citizenship is maybe the most important preventive step regarding educational institutions and its teachers/professors.

In other words, it is important not to just rely on formal education but to use non-formal and informal activities in schools to fight and prevent cyberbullying from a creative point of view.

On the other hand, parents "must demonstrate to their children through words and actions that they both desire the same end result: that the cyberbullying stops and that life does not become even more difficult."

How should parents react if they discover their own child is a cyberbully? Firstly, they need to explain to him/her how that behavior is provoking and inflicting harm and pain in the real world. After that, parents should be able to give him/her/them the opportunity to move on and end that behavior. Children need to know that every action, even if it is online, has serious consequences. From the parents' side, it is essential to start paying greater attention to their children's behavior and actions online.

1.3 Guidelines: How to deal with cyberbullying victims?
(Procedures, empathy, the importance of listening, emotional support, psychological support)

When you are a victim yourself:

If you are suffering from cyberbullying, we would advise following this series of steps:

- Seek help First of all, you need to talk, discuss with relatives or professionals!

- Report the content If the cyberbullying has been produced through a social network, report the content to that platform. This is not always effective, but it is important that the social network knows who the accused is so that they can take action, sometimes after several reports.

- Protect yourself Change your password, increase the privacy of your posts, remove personal information such as your email address, phone number or links to other accounts. As a temporary measure, **delete your account or change your nickname**.

#DigitSafe

- <u>Contact the Internet Service Provider (ISP)</u> Try to contact the Internet Service Provider of the person who is harassing you if they have been identified. The ISP can then contact the person or perhaps close their internet account directly.
- <u>File a complaint by going to a police station</u> Take evidence of the attack (for example, screenshots). The police will take note of your complaint and all the information related to your complaint and put it into a report.
- <u>Report the cyberbullying publicly</u> <u>S</u>hare screenshots of the bully (be sure to hide the bully's username and profile picture so that you are not accused of defamation).

As a teacher:

Teachers have to pay attention to different signs that can show that a child is being cyberbullied. Some of these signs can be a rapid increase or decrease in device use or an emotional response to what is happening on their device. If a child hides their screen or device when others are near and avoids discussion, this should be taken into account.

In addition, teachers also have to help kids how to identify, respond and avoid cyberbullying. Some guidelines would be:

- Communication is very important so if you ever think a child is being cyberbullied, speak to them privately and ask about it. You can also speak to a parent about it. Teachers can be a mediator between the child, parents, and school.
- Promote a safe class environment. Help children develop emotional intelligence so that they can learn self-awareness and self-regulation skills and learn how to have empathy for others.

#DigitSafe

- Encourage students to pay attention to signs that can help them identify when something happens on digital media that makes them feel uncomfortable, worried, sad, or anxious.
- Teach them to think before posting.
- Explain to students the three ways they can and should respond if they witness cyberbullying: if you support the target of the bullying, you are an ally, if you try to stop the cyberbullying you are an upstander and if you are a victim of cyberbullying you have to report it to an adult.

As a parent:

It is very likely for kids not to recognize that they are being cyberbullied because they might feel ashamed. It is very common for the youth to suffer silently. They may be afraid that parents will react by restricting their online access, they may feel embarrassed that they cannot take care of the bullying themselves.

For these reasons, if parents see any signs in their kids, they must take action immediately. First of all, try to talk with your child and listen to them.

#DigitSafe

Engage them in a conversation about what is going on in a calm manner. Take your time to understand exactly what happened and the context in which it occurred.

Once you know about it, offer comfort and unconditional support as cyberbullying victims often experience feelings of isolation. Show your child that this situation can be dealt with in a way that does not involve online retaliation. Make your child feel safe, it must be the foremost priority as well as letting your child know that it is not their fault.

After that, try to collect as much evidence as possible. Print out or make screenshots or recordings of conversations, messages, pictures, videos, and other items which can serve as clear proof that your child is being cyberbullied.

The next step is to contact the content provider since cyberbullying always violates the Terms of Service of all legitimate service providers. They should take action on this matter so that your child does not suffer from it again.

If the cyberbully is a classmate or goes to the same school as your child, you should notify the school as soon as possible since they might have rules for responding to cyberbullying.

Parents can also contact the police in case the previous steps mentioned do not help the situation to get better.
If it is necessary, try to seek counselling for your child. Children may benefit from speaking with a mental health professional. They might prefer to dialogue with a third party who may be perceived as more objective.

1.4 Prevention measures

There is no foolproof way to prevent a child from being cyberbullied. However, there are different ways to reduce the likelihood that they will be targeted.

First of all, it's important to use passwords on everything and not share these passwords with anyone.

Kids have to know that it is important to keep personal stuff private. They should never share their address, cell phone number, or email address online. They should be careful about sharing too much information about where they go to school, especially if they have friends or followers online that they don't know really well.

They also have to know that they have to log out when using public devices such as public computers or laptops at school or the library. This includes logging out of email, social media accounts, their school account, or any other account they may open.

Last, but perhaps most importantly, children should be aware that if they are ever the victims of cyberbullying, they must report it to their parents or teachers.

1.5 How to report cyberbullying
(Legal framework, institutions, NGOs, etc.)

One of the most significant aspects of reporting cyberbullying is that most European countries do not have specific legislation on cyberbullying.

Despite the importance, the large number of cases, and the concern among young people, legislation has not yet made progress in this area. This has made the work of institutions and organizations essential to help to identify cases, denounce them and give support to the victims.

#DigitSafe

2. Hate speech

2.1 What is hate speech?

There is no universally accepted definition of hate speech. In this section, we will outline a couple of definitions which are outlined in both EU law and by leading organizations combating hate speech.

....

- (Illegal) Hate speech is defined by EU law as '*the public incitement to violence or hatred on the basis of certain characteristics, including race, color, religion, descent and national or ethnic origin*.' Whilst the Framework Decision relates to racism and xenophobia, the majority of Member States have extended their national laws to include other grounds such as sexual orientation, gender identity and disability (5).

....

2.2 How to Prevent Hate Speech

One way to combat hate speech is to block and report accounts of hate speech that you encounter online (see the next section on tips on how to report hate speech). The United Nations recommend committing to following practices to prevent hate speech (6):

((5) Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016)
https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf
(6) United Nations- how to deal with hate speech? https://www.un.org/en/hate-speech/take-action/engage

#DigitSafe

- **Pause** - restrain from making any hateful comments yourself and/ or sharing such content
- **Fact check** - make sure that you spot false and biassed information before spreading misinformation
- **Challenge** - spread your own counter speech and challenge hate speech wherever possible
- **Support** - take a public stand and extend solidarity to targets of hate speech
- **Report** - check out the community guidelines of social media platforms you use and report instances of hate speech which violate these guidelines. For more serious cases you may wish to file a complaint with the police (e.g., when there is incitement to violence).
- **Educate** - share educational resources and public campaigns or start conversations with your friends and family
- **Commit** - consider joining an NGO or initiative that works to address hate speech within your community.

www.un.org/en/hate-speech/take-action/engage

#DigitSafe

2.3 How to report Hate Speech

Users can directly report any incidents of hate speech through the social media channel in which they encounter it. The council of Europe website provides information on how to report on social media channels. There are some cases whereby you do not need to have an account to report. For example, on Facebook you can complete this online form without having or being logged into a Facebook account.

Some European countries have introduced national reporting procedures and mechanisms for hate speech, hate crime and cyberbullying as part of the European Councils 'No Hate Speech Youth Campaign'.

Other suggestions for reporting hate speech include:
- Report the hate speech to the police.
- Report to an authoritative body for example, a civil or administrative court.
- Report to an NGO for example, MiND is the national reporting center in the Netherlands for hate speech and discriminatory content.
- Talk to someone you trust- e.g., a parent, friend, teacher.

3. Cybersecurity and Privacy

3.1. Why is personal data protection important?

The term personal data protection is defined in Art. 4 (1) of the General Data Protection Regulation: personal data are any information which are related to an identified or identifiable natural person. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. In the next paragraphs we will further explore the types of data that require protection.

Data protection is important, since it prevents the misuse of the information of an individual or an organization, it aims to prevent different privacy and security risks, such as fraudulent activities, hacking, phishing, and identity theft.

#DigitSafe

3.2. Types of personal data and privacy threats and crimes

1 **Identity theft**

Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finances, and reputation. The identity thief may use your information to apply for credit, file taxes, or get medical services.

2 **Online sexual harassment**

Online sexual harassment is defined as unwanted sexual conduct on any digital platform and it is recognized as a form of sexual violence. Online sexual harassment encompasses a wide range of behaviors that use digital content (images, videos, posts, messages, pages) on a variety of different platforms (private or public).

#DigitSafe

3 Phishing

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually performed through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves.

4 Internet fraud and scams

Internet fraud involves using online services and software with access to the internet to defraud or take advantage of victims. The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.

5 Greeting Card Scams

Many internet fraud attacks focus on popular events to scam the people that celebrate them. This includes birthdays, Christmas, and Easter, which are commonly marked by sharing greeting cards with friends and family members via email. Hackers typically exploit this by installing malicious software within an email greeting card, which downloads and installs onto the recipient's device when they open the greeting card.

6 Credit Card Scams

Credit card fraud typically occurs when hackers fraudulently acquire people's credit or debit card details in an attempt to steal money or make purchases. To obtain these details, internet fraudsters often use too-good-to-be-true credit card or bank loan deals to lure victims. For example, a victim might receive a message from their bank telling them they are eligible for a special loan deal, or a vast amount of money has been made available to them as a loan.

#DigitSafe

7 Online Dating Scams

Another typical example of internet fraud targets the excess of online dating applications and websites. Hackers focus on these apps to lure victims into sending money and sharing personal data with new love interests. Scammers typically create fake profiles to interact with users, develop a relationship, slowly build their trust, create a phony story, and ask the user for financial help.

8 Lottery Fee Fraud

Another common form of internet fraud is email scams that tell victims they have won the lottery. These scams will inform recipients that they can only claim their prize after they have paid a small fee.

#DigitSafe

9   The Nigerian Prince

The scam uses the premise of a wealthy Nigerian family or individual who wants to share their wealth in return for assistance in accessing their inheritance. It uses phishing tactics to send emails that outline an emotional backstory, then lures victims into a promise of significant financial reward. The scam typically begins by asking for a small fee to help with legal processes and paperwork with the promise of a large sum of money further down the line.

10   Spam

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

#DigitSafe

3.3. How to report cybersecurity threats on social media/institutions

All social networks have established mechanisms for reporting different types of cybersecurity threats, including online hate speech, identity theft, sexual harassment, cyberbullying, etc.

Below you can find information about some of the most popular social networks:

Facebook

- Facebook security issues have multiple categories. There may be an abusive content or hate page you want to report or maybe someone is impersonating you on Facebook, etc. The best way to report abusive content or spam on Facebook is by using the Report link near the content itself.

https://www.facebook.com/help

Twitter

- In the Help Center of Twitter you can find information and support in case of compromised and hacked accounts, about privacy, spam and fake accounts, sensitive and offensive content, abusive behavior and its reporting.

https://help.twitter.com/en

#DigitSafe

Instagram

- Report posts:

If you see a post, message or account you think goes against Instagram's Community Guidelines, you can report it. You can report individual pieces of content by tapping the three dots above a post, holding on to a message, or by visiting an account and reporting directly from the profile. For more information, visit Instagram's Help Center.

- Report accounts:

Accounts in violation of Instagram's Community Guidelines can be reported in-app or via a web form. For more information you can refer to the Help Center.

https://help.instagram.com/

TikTok

- For questions, concerns, or issues with your profile, you can find information and support by scanning the code below. In the section Safety you can go to Report a problem and report a LIVE video, a LIVE comment, a video, a comment, a direct message, a sound, a hashtag, and you can also report someone. The steps are very easy to follow, you just need to find the option Report and follow the instructions.

https://support.tiktok.com/en/

#DigitSafe

3.3. How to avoid security data risks

One of the most important things to do in order to keep our data protected is to have a strong password. It will be very useful since nowadays cybercriminals keep thinking of new and innovative ways to hack accounts and get ahold of personal data.

Additionally, in order to keep your information protected it is recommended to use only websites you trust. Many people do not know how to check if a website is safe or not, thus, some tips will be given.

1 First of all, check if the URL has the correct spelling, is secured with "https" and has some sort of indicator that it is verified, such as a lock sign.

2 Secondly, websites that look unsafe usually are. If the website owner is not investing in the appearance and user experience, they probably are not investing in the security of the site.

#DigitSafe

3 Thirdly, you must be able to check that there is contact information available as well as an accessible privacy policy. These are usually found at the very bottom of the homepage. Another useful tip is to read some testimonies and reviews for the site from other people so you can get to know experiences that other people had using these websites.

There are also other practices that can put digital security at risk such as using public WIFI. It is true that this service that some hotels and airports provide is free, but it does have a price.

These free WIFI hotspots allow hackers to position themselves between the person using it and the connection point, so instead of talking directly with the hotspot, people are sending their information to the hacker, who then relies on it.

How can individuals protect their personal data?

1 Secure your accounts

2 Protect your web browsing

3 Use antivirus software on your computer

4 Update your software and devices

5 Don't install software that you don't know and trust fully

6 Disable Bluetooth when not using it

7 Be overly cautious when sharing personal information

8 Watch out for impersonators

9 Don't share too much information on social networking platforms

10 Customize your social networking privacy settings

11 Don't forget to sign out

12 Don't open emails from people you don't know

13 Don't save passwords in your browser

14 Don't use social media credentials to register for or sign in on third-party sites

15 Choose a safe, reputable email provider

#DigitSafe

4. Conclusion

Throughout this handbook Cyberbullying and Hate Speech have been explained and contextualized. Their definitions can vary along different countries, however both of them are considered as an aggression to other people. In the case of Cyberbully there are normally three actors (the perpetrator, the victim, and bystanders), in the case of Hate Speech, it is harder to establish a common scenario, but it equally involves a person who discriminates and the receptor who is discriminated against.

This handbook includes different ways of identifying, dealing, and reporting cyberbullying and hate speech, of course, it will depend on who is the victim (yourself, a colleague, your children, etc.) but also on the legal framework of the country.

For example, in Spain you can report it to the police while in Netherlands there is a national discrimination helpline. In addition, it is shown why concepts like data protection or CIAD triad are important as well as types of privacy threats such as identity theft, online sexual harassment, phishing, or frauds.

#DigitSafe

In conclusion, this document does not only offer definitions or key concepts regarding cyberbullying and hate speech, but it also serves as a guide to prevent, react, and report these kinds of abuses.

#DigitSafe

Boosting digital safe spaces and resilience

Questions &
Information:

✉ **info@digit-safe.com**

🌐 **www.digit-safe.com**