



# Guide for online safety

Coordinator-Scoala Gimnaziala Zvoristea Romania

#### Collaborators:

Zespol Szkolno Przedszkolny nr 1 w Piszu, Poland Sanders School, United Kingdom Luis Carrillo De Sotomayor High School, Spain

The necessity of using this guide	3
Chapter I: Types of cyberbullying	∠
Chapter II: The benefits of using internet	. 12
Chapter III: Negative consequences of cyberbullying	. 17
Chapter IV: How to use the internet safely	20
Bibliographique ressources:	30

## The necessity of using this guide

This guide represents the results of our efforts in the European project Erasmus+ "Let's remove bullying and promote kindness to one another", having as partners Great Britain, Romania, Spain and Poland.

The main goal of this guide is to reveal theoretical resources easy to understand, underlined by the practical applications used by parents, teachers and especially by students, in order to use the internet safely.

After reading this guide, students will be able to do connections between principles, benefits but also social risks of using social media. They will also be able to react properly in cases of cyberbullying, knowing where they can ask for help and support in case of necessity. It is also important for them to know how to use internet in educational purposes.

The guide also contains the main negative consequences of cyberbullying, for children to realize the huge impact of such a situation on their psychological development.

## **Chapter I: Types of cyberbullying**

By cyberbullying we mean different forms of psychological abuse committed by acts harassment transmitted by harassment technologies information and communication, such as the Internet, mobile phone or wireless networks or Bluetooth. These are acts of violence and are being done for the purpose of threat, intimidation or insult victims. They have a repetitive character and can be committed by both individuals and groups of people.

#### For example:

- harassment, repeated offending of a people, using words mocking, obscene nicknames, humiliating images, transmitted via the Internet;
- ridiculing a child by creating a profile or blog in which they appear false or offensive information, photos transformed with offensive character;
- misuse and offensive use of the tag, especially in social networks, etc.; (identification of a person in a particular picture or post).
- malicious exclusion of a person from an online group or community;
- publishing private films or photos of a person without his consent;
- password theft to gain access to personal correspondence and forward in the name of the victim compromising messages;
- intentional sending of a message infected.

Kids and teenagers are incredibly prone to cyberbullying every very often.

Cyberbullying is a major issue in today's digital age. The cases are increasing because of the excessive use of social media and the internet. Parents and teachers must take action to protect their children from getting bullied.

Before knowing the solutions for this matter, we should have in attention the different types of cyberbullying. It will help parents and teachers to find out if their children are already facing cyberbullying.

#### Harassment

One of the main types of cyberbullying is online harassment. It contains a huge part of the cyberbullying attacks as it refers to hurtful messages, threats, and constant online insult and intimidation. Harassment refers to aggressive and intentional bullying by sending threats to the victim. This type of cyberbullying can cause massive harm to the victims. It may lead to depression, anxiety, and dramatic situations.

Harassment online can record a higher gravity in comparison with face-to-face harassment. The aggressor takes advantage of the relative situation of anonymity on the Internet, committing actions on who would not have committed them otherwise. His superiority on the victim is not of a physical nature, but of a technical nature, much easier to exploit. In addition, the aggressor underestimates the effects, considering the actions a simple fun.

Information posted online persists, their existence being relatively permanent, difficult to be eliminated, sometimes impossible.

Abuse has a strong invasive character, with negative impact on the entire personal life of the victim, at school or at home, online or offline, with a spread that is difficult to control. Signs of online harassment:

- not participating in the debates organized in school;
- drastic decisions, for example, meeting at a sport practiced for many years
- negative self-perception, depression, anxiety, nervousness;
- suicidal thoughts (educators must announce immediately parents and school psychologist if they notice a strange behaviour)

#### **Cyberstalking**

Another type of cyberbullying is cyberstalking. A bully who cyberstalks someone can monitor the victim online. They can see the victim's digital activities such as posts, comments, views and others. Cyberstalked can also lead to offline stalking.

Victims of cyberstalking can develop anxiety, fear, inferiority, and insecurity.

#### **Fraping**

"Fraping" is a term that originated from "Facebook" and "raping." From its name itself, fraping it's about an unconsented posting on Facebook using the victim's profile and it might lead to ruining the victim's online reputation.

For example, a child who forgot to log out the account and someone used it to post something improper, and then it is an example of "fraping" or Facebook raping.

#### Masquerading

Cyberbullies become braver if they use fake accounts to attack their victim and that's why this kind of cyberbullying falls as the masquerading.

The bully might create a new profile using a fake email address, fake social media account, and fake photos. They can also fool someone using this account and try to impress the victim. Another masquerading type is when the bully tries to play the victim using their new fake account. They will tend to target someone and do destructive acts using these fake profiles.

The parents must talk to children to remind them not to post any personal information and photos online. They can also make their accounts private so they can hide any personal information or photos.

#### Outing/Doxing

One of insulting act under cyberbullying is outing or doxing. It refers to humiliate and embarrass the victims. The bully can expose personal photos, documents, conversations, and intimate details without the victims' knowledge.

In this case, the victim will be surprised by finding out that their things are already available online the central issue in outing the victim's lack of consent.

Sometimes the cyberbully is inside the private group from where the victim told a secret. Then, the cyberbully uses this information to humiliate the person.

It is important to make children understand that their personal lives are very different from their social media accounts. Parents need to remind their children to think first before sharing something personal online.

#### **Trickery**

Trickery is in a way similar to outing or doxing. The only difference is that the cyberbully is a stranger, not a friend.

In trickery, cyberbully can create a new fake account and try to be friends with the victim. Once they get the victim's attention and trust, they will begin to ask questions and encourage them to talk about personal information. Finally, cyberbully can spread other people's secrets or even post them online.

To prevent trickery, parents have to teach their children not to talk to strangers, even if they look nice. They can also check their accounts regularly to see who they are talking or communicating online.

#### Dissing

Dissing refers to an online attack on someone with close relationships with the victim. They use private messages or public posts to ruin his reputation. They could spread cruel details, inappropriate images or even false news about the victim and the victim's family.

In addition, dissing can also lead to damage to the victim's relationship with other people. Spreading information online to tarnish the digital image of friends, families and their followers is an act of dissent.

The cyberbully can use pictures, videos, and screenshots of your online activities and use them to tear you down.

#### **Trolling**

In addition to posting, tough comments on social networking accounts is another way of cyberbullying. Cyberbully may flood you with ironic comments or even introduce harmful content to your account. It could intentionally upset friends and followers of social media through these tools.

Trolling cyberbullies don't have any personal relationship with victims. So, they are more aggressive in breaking posts and personal profile.

Facebook and other social networking accounts have included privacy settings so that others do not jump into your child's accounts. Parents must apply these security measures to protect their children's online reputation.

#### Flaming

Flaming is similar to trolling, but cyberbully tries to attack the victim directly. They could post and send direct threats, insults and offensive messages. Cyberbully can also start an online fight in which the victim will be harshly attacked. It could be a real deterioration in emotional values.

#### **Exclusion**

Another dangerous act of cyberbullying is exclusion. In this type, cyberbully will explicitly show that the victim's group does not invite the victim into social groups. The bullies could use message or conversations, stressing that they will not include the victim.

Exclusively it's like leaving someone behind. It can cause emotional embarrassment to the child or even feel expelled.

#### The role of the school in prevention and removing online harassment

School becomes responsible for developing a culture of protecting students against violence of any kind, physical or online. Schools are encouraged to develop their own plan anti-cyberbullying including actions information for the prevention of acts of online aggression and detection procedures and elimination of harassment between students.

An anti-cyberbullying plan must contain the following strategies for creating friendly relationships and non-violent among students:

- emotional support and protection provided victims;
- encouraging other students to support victims;
- organizing free discussions, debates between students, educators and parents looking use of ICT;
- assistance provided to aggressors to understand the negative effects of their actions;
- parental involvement.

#### **School activities**

## 1. Let's remove Bullying!

Learning Objectives

- Students will learn about the different types of bullying.
- Students will discuss different ways to bully.
- Students will create a definition for bullying.

Breaking ice activity: Name train (5 minutes)

One Student walks around the group and picks one Student. That Student then puts their hands on the leader's shoulders and yells their name in whatever tone they want, and everyone else has to mimic it. The leader keeps dragging the train around while the last student to join picks someone else.

#### Activity 1

Watching a video (5 minutes)

Procedure

• Teacher selects a video that is appropriate and interesting for students regarding cyberbullying: <a href="https://www.youtube.com/watch?v=rgMwh5Fnp3I&ab\_channel=UNESCO">https://www.youtube.com/watch?v=rgMwh5Fnp3I&ab\_channel=UNESCO</a>

Students watch a video showing types of bullying, its effects and ways of intervention in these situations.

#### Activity 2

Awareness Activity (30 minutes)

Procedure

Part A (20 minutes)

- Teacher divides the class into teams (3 5 students work well). Teacher gives each team a set of index cards and tells them they have 10 minutes to come up with as many different ways that people bully as possible. Students will write each reason on each index card.
- When the 10 minutes is up, teacher hands each group one of the "Bullying What is it" handouts. Teacher tells them to divide the ways people bully into the categories on the handout. After this, Students will create a definition of bullying and write it in the square on the handout.
- Teacher has some or all of the groups share their definitions for each type of bullying.

#### Part B (10 minutes)

- Teacher divides everyone into eight teams and has each team draw one of the "Why We Bully Cards" from a hat. Teacher gives the groups 2 minutes to come up with short role play that illustrates what's on the card. The other teams have to guess the "reason" that the person is bullying. The first team to guess the reason gets 5 points. When all teams have done their role play, teacher has a lightening round where each time calls out reasons not to bully. Each original reason that is stated wins the team 10 points. The team with the most combined points wins.
- Teacher helps when necessary.

#### Activity 3

Wrap Up & Processing (10 minutes)

- When asking the questions, teacher allows time for group members to answer. He tries not to rush the processing and gives everyone time to think about what they have learned.
- A. What have you learnt about the topic of bullying today?
- B. Can you think of times in your life when you or someone you know was bullied?
- C. How do you think being bullied makes people feel?
- D. If you or someone you know is being bullied what are some things that they can do for help or to stop the bullying?
- E. If someone started bullying you, who would you talk to about the situation? Who are some of the people that would help you?
- F. What does it mean to be a bystander? Why are some people bystanders when it comes to bullying? How can you go from being a bystander to someone who helps the situation?
- G. Now that you know more about bullying what do you think you can do to make a difference at school? What are some ways that you could help someone who was being bullied?

#### Activity 4 (5 minutes)

Teacher asks students to create posters containing drawings and impact images to raise awareness about bullying.

#### 2. "Bullying is not a solution; friendship is the way!"

#### **PURPOSE:**

Correct information for primary and secondary school students, their parents and teachers on the phenomenon "bullying": definition, forms of manifestation, causes, effects, statistics on the degree of escalation of the phenomenon in the Romanian school, forms of prevention, ways to take action, to intervene for themselves and / or for others, in order to reduce the number of such cases.

#### **OBJECTIVES:**

- raising children's awareness of the consequences resulting from the application of aggressive and antisocial acts;
- development of appropriate social behaviour (in relationships with colleagues and teachers) by familiarizing them with various rules of positive and civilized conduct, in relation to one's own person and to others;
- creating a state of awareness of children for a society based on anti-bullying behaviours, in the school and family context;
- mastering by students, their parents and teachers, techniques for the correct management of situations in which students are victims of people who practice "bullying".

#### **ACTIVITIES:**

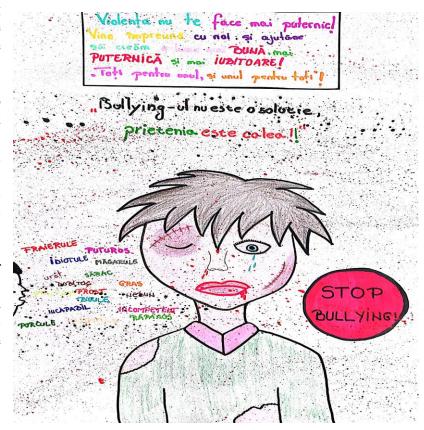
- 1. The phenomenon of bullying, forms and causes presentations, debates.
- 2. How can bullying affect a child's life? case studies, role-playing games.
- 3. Mediation of conflicts in and out of school exposures, debates on acquiring emotion management techniques, ways of acting in the event of aggression, adoption of positive, tolerant attitudes, empathic, avoiding verbal and physical aggression, marginalization and discrimination, harassment and online threat.
- 4. My anti-bullying message-collage workshops, posters, containing messages and thematic drawings, videos.
- 5. Act, don't be indifferent! explanation of principles of intervention in the case of aggressive students.
- 6. Together we can make the world a better place! promoting moral, social and cultural values.
- 7. The activities aimed to identify effective solutions to prevent and combat the phenomenon of violence in the school environment. Also, reporting cases from parents contributed to the involvement of students in this project.

Students showed interest in this project, being actively and creatively involved, finding a suitable environment to signal different forms of bullying that they have experienced or identified in their colleagues. Thus, they had openness to debate concrete examples of forms of bullying, they were

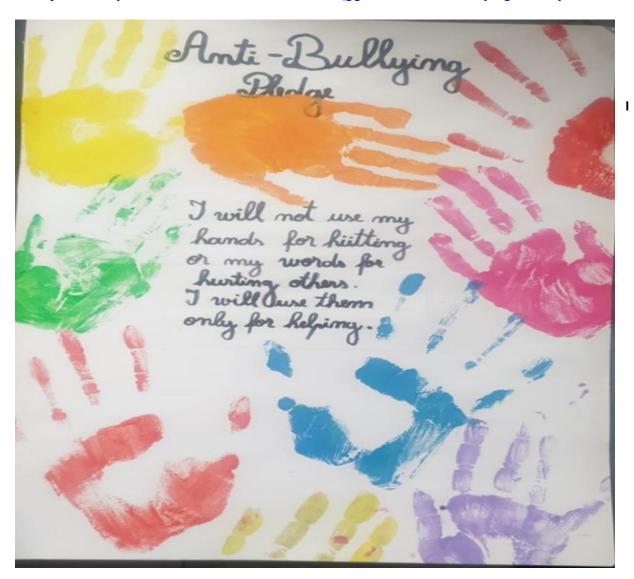
involved in case studies, role-playing games to expose their emotions, the mode of action and the attitude shown in these situations.

Together with the teachers involved, the students were able to identify emotion management techniques, recognize positive, tolerant, empathic attitudes stressed the importance of avoiding verbal/physical aggression/online threats, giving free rein to these feelings, feelings drawings, posters, recorded messages that they then passed on to friends or the community.

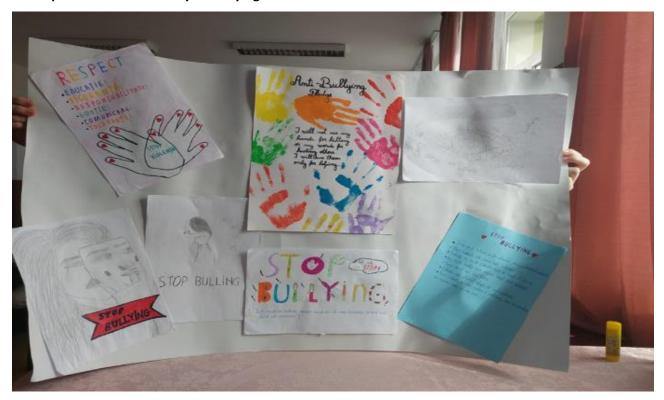
In the end we gathered everything, making a representative poster and a video chosen with the students.



https://www.youtube.com/watch?v=F6r0B78GQgg&ab\_channel=Bullying.NoWay%21



can prevent and combat cyberbullying!



#### Activity to prevent and combat the phenomenon of cyberbullying

Target group: secondary school students

Purpose:

To develop the skills of teenagers to identify cyberbullying and to act effectively to prevent and combat cyberbullying situations.

#### Objectives:

- developing students' skills to identify the defining elements of virtual aggression;
- developing students' skills to identify the best strategies to prevent and combat cyberbullying;
- developing students' abilities to reflect on the causes and the consequences of aggression in the virtual environment;
- developing students' abilities to reflect on the consequences cyberbullying and act accordingly.

Procedural resources: practical activities, group activities, pair activities, individual activities, debates, case study.

The description program:

Through this program, teenagers will discover a series of strategies and methods of act to identify, prevent and combat cyberbullying.

The program is designed to enable, through practical activities proposed to students, and analysis of the causes and consequences of cyberbullying, but also the analysis of concrete cyberbullying situations. Also, the program allows the realization of a site of all content elements from session on cyberbullying. Each participant have to reflect on what he understood from the topic addressed, on what was useful and interesting, but also to future plans regarding effective ways to prevent the development of negative consequences of cyberbullying.

#### Activities

- 1. What is cyberbullying?
  - a. to identify the forms of manifestation of cyberbullying;
  - b. to identify the virtual environments of manifestation of cyberbullying;
  - c. to build their own definitions of cyberbullying, based on debates and analyses during the activity;
  - d. to reflect on the realities related to cyberbullying.
- 2. What we know and what we don't know about cyberbullying!
  - a. to analyse the statistical data related to the incidences of the phenomenon of global cyberbullying;
  - b. to identify possible causes of the presented situations;
  - c. to reflect on the realities related to violence in the virtual environment, on its causes and consequences.
- 3. How can we combat cyberbullying!
  - a. to analyse strategies to combat cyberbullying;
  - b. to create a top (from 1 to 7) of the most effective strategies presented and analysed;
  - c. to argue the options regarding the selection of the most effective ones strategies.
- 4. Consequences of cyberbullying
  - d. to analyse the cyberbullying cases presented;
  - e. to identify the causes of cyberbullying from the situations presented;
  - f. to identify the consequences of cyberbullying from the situations presented;
  - g. to identify ways to combat/ prevent cyberbullying from the situations presented.
- 5. Similar story...
  - a. to describe a situation in which he experienced a form of cyberbullying;
  - b. to describe a situation in which he witnessed a form of cyberbullying;
  - c. to reflect on the ways of confronting the situations of cyberbullying.
- 6. Now I know about cyberbullying...
  - a. write down what he knows about cyberbullying;
  - b. to write down what they would like to know more about cyberbullying;

- c. to write down hopes and expectations related to combat and prevention the phenomenon of cyberbullying;
- d. to constantly reflect on the phenomenon of cyberbullying.
- 7. Be active! Create a message for your classmates!
  - a. write an essay describing concrete action strategies to prevent and combat cyberbullying;
  - b. to create an impactful poster in the fight for prevention and combat cyberbullying;
  - c. to design a slogan/ message to combat cyberbullying;
  - d. to create a website with informational material about cyberbullying.

#### **Examples of educational activities**

**Brainstorming** can be a method that can be used for introduction to the theme. Children can be grouped into teams and receive as a task to write on common lists everything they know about the bullying phenomenon. Then there are discussions in small groups and then at the class level to decide what is relevant and what is not.

Role-playing games have clear sets of rules, students are advised not to disclose personal information, not to use their own name in roles, behaviour must also be mediated, no student is allowed to strike or use insulting words. You can choose certain specific bullying situations, then the actors, their fictitious names and play the scenes in front of the class. It is very important in these exercises to discuss immediately after the interpretation, how each of the actors felt, being a victim, an aggressor or a witness. It is very interesting here if a child who has acted as an aggressor in real life is chosen as a victim, if possible, in order to be able to see the situation from another point of view.

An impressive **exercise** is the **drawing of a child's figure on a large sheet**, which is cut on the contour and attached to the sheet with adhesive tape only at the top. Children are given the theme of thinking of an insult or an offensive word to the silhouette on the board, not to say but depending on how painful it is to break part of the figure (a finger, a piece of the foot, etc.) to keep on the bench, with the mention that they will use it a little later. It starts in order, from one end of the class, until it reaches the other and all the students pass one by one at a time to the silhouette on the board. They can colour the piece on the bench but are asked not to write words. It returns in reverse order to glue the broken pieces with adhesive tape, one by one, one until the figure is restored.

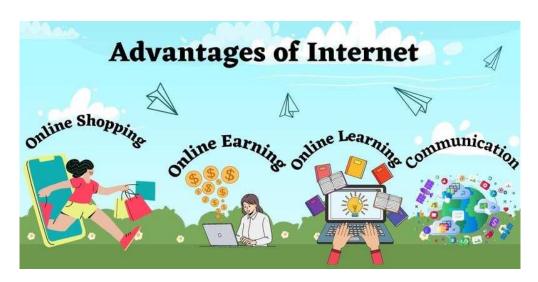
In the end, children are asked to express their opinion on whether the figure looks the same as before this process, whether or not what we do has consequences. They are invited to say how they think someone who is assaulted a large number of times, if the wounds heal, if the scars are seen.

These exercises make children more empathic, look more closely at what is happening around them and no longer tolerate aggressive behaviours in the school environment.

## **Chapter II: The benefits of using internet**

- 1. Fast and convenient communication.
- 2. Access to virtually knowledge from around the world.
- 3. Finding people with similar interests.
- 4. Convenience in everyday functioning, e.g. shopping.
- 5. Social networks.
- 6. Possibility of conducting remote lessons.
- 7. Access to online teaching materials.
- 8. Possibility of remote work.
- 9. Online courses
- 10. Entertainment.
- 11. Social actions.

Other benefits of using internet and social media are: searching information, sharing experiences, meeting new people, talking with everybody in the world, learning new things, discovering other countries, cultures, languages, lifestyle, sharing and comparing ideas, saving paper, entertainment, searching and applying for jobs, creating work and art, business communication, creating a better world, making online payments, finance and banking, online shopping, playing videogames, maintaining family relationships, saving time and money by making video conferencing, providing better access to health information and options, promoting workforce development skills, decreasing isolation and loneliness, watching or downloading music, movies or tv-shows.



In the ever-evolving landscape of education, the internet stands as a formidable ally, revolutionizing traditional paradigms and ushering in an era of unprecedented opportunities.

As we embark on this educational odyssey, it becomes evident that the advantages of incorporating the internet into learning environments are vast and transformative.

Access to a Wealth of Information: The internet, a digital repository of human knowledge, has democratized access to information. Gone are the days of being tethered to static textbooks; the internet provides a dynamic and expansive platform where students can delve into a treasure trove of information. From scholarly articles to interactive tutorials, the wealth of knowledge available empowers learners to explore subjects in depth, fostering a spirit of intellectual curiosity.

Global Connectivity and Collaboration: Education is no longer confined to the physical boundaries of classrooms or institutions. The internet has woven a global tapestry, connecting students and educators across continents. This interconnectedness fosters a rich cultural exchange and collaboration on an unprecedented scale. Through online platforms, students can engage in real-time discussions with peers from diverse backgrounds, broadening their perspectives and preparing them for the globalized world that awaits.

Interactive and Engaging Learning: The advent of online learning platforms has transformed education into a dynamic and interactive experience. Multimedia resources, such as videos, simulations, and virtual labs, enhance the learning process by catering to different learning styles. The internet's multimedia capabilities make complex concepts more accessible, ensuring that students can engage with content in ways that resonate with them, leading to a deeper understanding and retention of knowledge.

**Personalized Learning Journeys:** The internet facilitates personalized learning experiences tailored to individual needs and preferences. Online courses and educational platforms allow students to learn at their own pace, ensuring mastery before progressing to the next level. This flexibility is particularly beneficial for diverse learning styles and accommodates the varied pace at which students absorb and assimilate information.

**Real-world Application through Digital Resources:** The internet serves as a gateway to real-world applications of theoretical concepts. Digital resources, such as case studies, industry reports, and interactive simulations, bridge the gap between theory and practice. Students can explore the practical implications of their studies, gaining insights into how their acquired knowledge is relevant and applicable in professional settings.

**Continuous Learning Opportunities:** The internet ensures that the pursuit of knowledge is not confined to the constraints of time and space. With a plethora of online courses, webinars, and educational resources available 24/7, individuals can engage in continuous learning. This democratization of education enables professionals to upskill, stay relevant in their respective fields, and adapt to the ever-changing demands of the job market.

**Promote student research**. The main advantage of widespread access to the internet is the ability to do your own research and inform yourself more than you ever could in the classroom. The internet is the largest library, and students should learn how to properly navigate this modern information centre to be able to separate the wheat from the chaff when it comes to information. The internet is also a great place for discussions and polls, both of which could be very valuable in an academic situation. Computer literacy is a necessary ability for the future, so promoting independent online research is the key.

**Flexibility**. The internet was designed with flexibility in mind, it can run anywhere, and basically everyone has access to a mobile phone nowadays. Therefore, you can inform yourself in a variety of ways and contexts, from the classic, trusty academic sources to podcasts, documentaries and videogames.

**Anonymity**. Due to the anonymous nature of the internet, anyone can share whatever they wish, with very little fear of censor or repercussions in the real world. Consequently, the internet is a safe haven for journalists or others wishing to show the harsh realities of the world and a thorn in the side of any real-life malefactors.

#### Social media in the classroom

#### 1. Use a Facebook Group

Facebook can be the perfect social media platform to incorporate into the classroom.

Teachers can use it to post class updates, share homework assignments and encourage discussions.

Each social media platform offers many different ways to be used in the classroom, from sharing announcements to holding live lectures, and so much more.



#### 2. Use a Facebook Group to stream live lectures and host discussions.

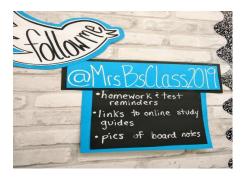
Teachers can also create Facebook Groups for each of their classes - both public or private - and stream Facebook Live lectures, post discussion questions, assign homework and make class announcements.

Email both parents and students a direct link to the Facebook Group for access.

#### 3. Use Twitter as a class message board.

Twitter can be great as a discussion board or message board for a class. Teachers can create a single Twitter handle per class and reuse it every year, or they can create a new handle each school year.

Teacher can use Twitter to post reminders for assignment due dates or share inspirational quotes and helpful links to practice quizzes or resources.



Teacher can also create discussions and Twitter chats surrounding a specific hashtag that they create.

#### 4. Use Instagram for photo essays

In a visual heavy class, students can use Instagram to present a series of photos or graphics in a visually appealing manner. Instagram allows students to practice digital storytelling in ways that other social media platforms may fall short.



Students can create class-specific Instagram accounts and may delete them after the course is over if they so choose.

#### 5. Create a class blog for discussions.

There are many different platforms available, such as WordPress, SquareSpace, Wix, Blogger, Tumble or Medium, where teachers can create a class blog. Students can create their own user accounts to make discussion posts or add comments on class prompts.



#### 6. Assign blog posts as essays.

Having students create in their own blog for essays or short-form writing is another strategy for combining social media and learning.

#### 7. Create a class-specific Pinterest board

Pinterest is a great social media platform for teachers to use to prepare and organize resources, lesson plans and worksheets for their classes in one place.



Pinterest can also be useful for students to curate a digital bibliography for research projects, papers or group assignments.

**8.** Using the educational platform like Google Classroom, that teachers and students can use for teaching and learning.

#### 9. Include social media links on your school website

Make it easy for parents and students to find your school's social media profiles by adding links to the website's main navigation or creating a social media directory that houses them all in one place.



## 10. Share school events and photos.

Highlighting events and extracurriculars can make your school stand out from the rest.





## Chapter III: Negative consequences of cyberbullying

## A. Causes of cyberbullying - where do the aggressors come from online and where do the victims come from?

Why does online violence occur? Who is responsible for it and why do others fall victim to it? It is difficult to answer this question unequivocally. Environmental and personality factors are often responsible for being the perpetrator and victim.

The perpetrators of violence are most often people:

- 1. with low self-confidence, who compensate for their low self-esteem by inflicting violence;
- 2. brought up in violent, pathological families or with the problem of excessive strictness of guardians;
  - 3. with sociopathic tendencies, taking pleasure in causing others pain.

#### Victims of this form of violence are most often people:

- 1. not very mentally resistant, with low self-esteem, submissive;
- 2. looking for friends and entertainment online, having difficulties functioning in the real world:
  - 3. shy, insecure, having difficulties with assertiveness and defending one's opinion.

In this case, cyberbullying is similar to traditional bullying: the perpetrator is a person with problems or a sociopath. The victim is a submissive person, complexed and not very self-confident. Unfortunately, in this case the perpetrator may also be someone similar to the victim: shy and quiet, who takes on the role of the aggressor in the virtual world.

## **B.** Negative effects of cyberbullying:

## Psychological effects of cyberbullying - how to help victims?

Online violence does not leave any marks on the body, which does not mean that it has no consequences. The effects it may have on its victims are usually only noticeable after some time and include:

- 1. experiencing negative emotions: fear, anxiety, anger, frustration
- 2. feeling of helplessness
- 3. loss of self-esteem and self-confidence
- 4. problems with sleeping and concentrating
- 5. intensification of social isolation
- 6. neglecting one's personal and professional duties
- 7. depressive moods
- 8. thoughts or even suicide attempts.

Much depends on the characteristics of a given person: victims may react differently to cyberbullying and its effects may be diverse. Victims of cyberbullying may or may not require help. In many cases, support in the form of periodic psychological therapy is implemented. When cyberbullying has been long-term or very advanced, depression or other disorders are suspected, the victim is referred for psychiatric examination.

The perpetrators of cyberbullying also have long-term consequences: their aggressive behaviour becomes stronger, their sense of responsibility for their own actions decreases, and their tendency to engage in antisocial behaviour in the future may increase.

Beside the well-known advantages, the using of internet can cause informatics criminality, online addiction and also spreading of misinformation and problems connected to privacy, depression, feeling of scary, lack of communication, thoughts of suicide, isolation, health problems, loosing self-esteem, wasting time, losing relationships, overthinking.

Informatics criminality and security problems: Internet facilitates the robbery of personal information, of identity or threatening of security.

Online addiction and dropping of social interaction: this kind of addiction and the excessive using of internet can lead to less social interaction and this implies problems such as loneliness, depression and social isolation.

Spreading of misinformation and fake news: Internet became a platform of spreading misinformation and fake news and this implies confusion and loss of self-confidence. It's more difficult to distinguish the credibility of certain information when it is easy to spread on internet.

Issues connected to confidence and losing of personal data: Internet allows to organizations to



keep big amount of personal data that can be vulnerable to piracy. It permits to follow and create new profiles constantly, and this could be considered a violation of privacy.

The negative effects of using the Internet in children's lives has become a greater challenge. The extraordinary fast speed with which technology develops and implicitly the Internet is an advantage, but as time goes by, we unfortunately realize the destructive character it can have for all of us, but especially in the lives of children.

Children in particular can become captives in the mirage of the Internet and can often become victims either through applications, games or virtual dialogues with unknown people and in this way becoming very vulnerable victims. That is why the time spent in the virtual environment must be limited as much as possible.

Social networks have both advantages and disadvantages. They facilitate communication between people, but their use can also bring risks: children can become victims of aggressors, traffickers, people who wrote false information, when the child comes into contact with people with hidden intentions.

Like any form of bullying, cyberbullying also causes mental health disorders among children and we can expect negative effects such as: loss of interest in favourite daily activities (reading, playing, walking, outdoor activities), sleep and eating disorders, various health problems, drop in school results or other extracurricular activities, anxiety disorders or even depression.

According to UNICEF, the long-term negative effects of cyberbullying can affect in several ways:

- a). Mentally, the child may feel:
  - Angry
  - Embarrassed
  - Stupid
  - Really angry
- b). Emotionally, the child should be:
  - ashamed
  - anxious
  - agitated
  - disinterested in school or other activities

- socially isolated with a feeling of loneliness
- with a defensive attitude
- c). Physically it can be:
  - tired, even having insomnia
  - with symptoms such as headache, neck, stomach, eye pain caused by excessive exposure to monitor light
  - with poor personal hygiene
  - fluctuating in terms of weight, especially gaining weight because he no longer moves and does not feel the need to go out or play in his free time
  - sedentary

The suffering of children bullied in the online environment takes various forms, from the most diverse and unpleasant, such as:

- isolation
- sadness
- low self-esteem
- failure or even dropping out of school
- sentimental loneliness or exclusion
- depressive or anxious states

### Chapter IV: How to use the internet safely

The Internet is an excellent tool! Thanks to this, you can have fun, inform or communicate with friends. But it is also a world full of traps. To use it well, you have to be careful.

What are you risking? First, to be manipulated through fake news, false information circulating on the Internet that looks real! You can also catch viruses, computer programs that sneak into your computer. Or it stumbles upon images or videos that make you uncomfortable.

Safe internet browsing is not just a matter of technology. Attention and mistrust must accompany you and warn you to benefit, limiting the risks, resources and functions provided by the Internet.

When students use the internet, they are (often unknowingly) exposing to a wide range of potential online threats. Here is a list of just some of the biggest internet dangers you and your family need to take care of: identity theft; data breaches, malware and viruses; phishing and scam emails; fake websites; online scams; romance scams; inappropriate content; cyberbullying; faulty privacy settings.

Technology is an important tool for teaching and learning. Schools and families have to work together to help children learn to use technology safely and respectfully. Everyone has a key role to play in keeping children safe and secure when they are online.

Not only strangers can make children feel uncomfortable. Cyberbullying refers to cruel or intimidating messages sent online. These could be from former friends or other people you know, can also be sent anonymously in other words to a website where everyone has a screen name, so that people who are bullied may not know who is bullying them.

On social networks, malicious people may try to contact you by posing as friends.

There are some good practices to use the internet safely:

- Change passwords regularly.
- Use strong passwords.
- Check the privacy settings on social media.
- Give yourself a digital break!
- Don't provide personal information.
- Only use a legal operating system.
- Keep your browser and operating system updated
- Secure your router and don't use public Wi-Fi networks.
- Only use trusted networks.
- Use antivirus software.
- Don't open suspicious emails.
- Visit only safe sites.
- Beware of spam.
- Be careful when making friends.
- Create backups.
- Be careful what you post online.
- Don't act on emotions.

#### Other rules to keep in mind are:

- 1. Don't talk to strangers. Although it seems friendly, a person you only know on the Internet could have bad intentions.
- 2. Do not offer personal information. Your name, the school you study at, your photos are personal data. Here are some questions you need to ask yourself:
  - Do I know this person who wants to communicate with me in real life?
  - Do I want to share my personal information with a stranger?
  - Can I talk to him like my classmates, tell me my life, my daily life?
  - I'm posting a picture: what does it say about me?

Provides information that can find or identify me (street name, number from home, easily identifiable sports courses, school names...) can serve as a basis for a possible harasser (my physique, my origins, my beliefs, etc.).

- Am I allowed to post photos where my friends see each other?
- Did I ask their permission or that of their parents if they are minors?
- What are my risks?
- 3.Passwords are secret and don't forget them. Take care of your accounts with secure passwords that only you know and don't share with anyone.

Your password could be any combination of letters, numbers, and symbols. Accents and accented characters aren't supported.

- 4. When you're on a website, try to remain as anonymous as possible. That means keeping all private information private. Private information that you should never allow the public to see are:
  - your full name;
  - any type of photograph;
- your current location (some phones have automatic GPS apps built in that may need to be turned off);
  - home or school address or the address of any of your family or friends;
  - phone numbers;
  - social Security number;
  - passwords
  - names of family members
  - credit card numbers.

Most trustworthy people and companies won't ask for this type of information online. Always check with a parent if you are unsure, especially when shopping online or signing up for a website or app. Protecting your identity on the Internet you don't attract the negative attention of cyberbullies or cyber criminals. You are also less likely to be targeted by hackers or suffer from identity theft.

- 5. When sending messages or using video applications, use a pseudonym different from the screen name. If you ever find yourself in a conversation that makes you uncomfortable, you can go out without having to worry that someone knows your screen name and can follow you by e-mail.
- 6.Periodically, search your name on search engines to see what images and information come up for public. Quickly, adjust your privacy settings, change your passwords, and get in touch with the right platform if you see your sensitive information published online.
- 7. If someone or something upsets you or makes you feel uncomfortable you can always stop the chat or browsing and talk to your parents or specialists. If you get these bullying messages online, it's better to ignore them than answer them. Cyberbullies, just like other bullies, is looking for attention or a reaction. Besides you never want to provoke bullies. By ignoring them, you can take away their power. Cyberbullying can set off a lot of emotions. It's important you don't panic or fight back as sometimes that can make things worse. You also can try to delete or block bullies so that you no longer see their texts.
- 8. Take care of your reputation. Before you post something online on a social media platform, think about whether you want that information to be accessible to everyone. Don't forget that the internet is a public place.
  - 9. Respect others on the Internet. Treat everyone as you would like them to treat you.

When interacting with someone through social networks, forums or other online platforms it is important to be aware of your own language and behaviour, as well as to recognize when you or others are badly treated online. Acknowledge and accept others' ideas, culture. Respect others trust and confidentiality. Bullying, harassment, trolling and stalking are never OK. Check your mood! Are you feeling upset or angry? Then it's not the time to be messaging or posting on a social media site. People don't always make good decisions or think right when they're stressed out or upset. If you have to, call someone or go for a walk before you start venting online.

- 10. You can block and report that person. You can report the cyberbullying to the game, site or app it occurs on. Usually, cyberbullying is against their terms and conditions of use and should be removed (do this after you've taken screenshots).
- 11. Take screenshots. It's important to keep the evidence if you have to report. If keeping these saved are bad for your mental health, send a copy to someone you trust and then delete your own copy.

- 12. Protect your computer. Install a good antivirus and update it regularly. This way you will be safe from viruses.
- 13. If you pay for a purchase, check that you do it on a secure site whose address begins with  $^{\circ}$  which with a simple "http" (so without s), it means that the web page is not secure.

Try to shop only on reliable online shops, and preferably on sites you know. If you have any doubts about the reliability of an online store, a simple search on a search engine will allow you to find consumer comments on the service offered, on the quality of products.

- 14. Be careful what sites you enter. There may be disturbing images or false information on the Internet.
- 15. Ask for help when you feel unsafe online! Talk to parents about what is happening on the internet.
  - 16. Be safe and trust the websites!
- 17. Don't click random links, don't show your face, don't reveal your address and never use your real name.
  - 18. Keep chats private.
  - 19. Never put your bank card details on a sketchy website.
  - 20. Don't give your phone number!
  - 21. Don't reveal your daily life!
- 22. Don't meet in real life with people you chatted online! Keep friends online in the virtual world. Meeting friends online face to face presents more risks than other types of friends, because it's so easy for people to pretend to be something they aren't when you can't see or talk to them personally.
  - 23. Don't use the same password on all your accounts or devices!

Using the same password leaves your information vulnerable to financial and identity theft, so it is important to use a single one for each of your accounts.

Using that password will also leave your information vulnerable to financial theft and identity theft, it is often important to use the only one for the safety of DVDs.

- 24. When you're out keep your devices secure. Don't let other people use your phone unless you're with them, turn your laptop or tablet off when you're not using it. Don't let other people to get a look at your personal information.
- 25. If you don't recognize the sender of a document or file that needs to be downloaded, delete it without opening it to avoid getting a virus on your device. Virus protection software is required for every computer and should be updated periodically.
- 26. Even if email is relatively private, hackers could still access it or add you to their spam lists. Spam, like harassing or offensive notes, is annoying. But spam blockers can keep your mailbox from getting clogged. Many service providers will help you block out or screen inappropriate emails if your parents agree to set up age-appropriate parental controls.

#### Guidelines for schools to monitor online activity and mobile use

Throughout his school and extracurricular activities, the student develops digital skills like reading, writing, speaking, speaking, and games. It is important that teachers can identify with him the rules of caution to help him protect himself at-risk situations. Students should also know that they have rights and that they can exercise. When they are very young, they can get help from their parents.

Exposure to the Internet although it is useful can be dangerous for children and adolescents if its use is not well controlled. Hyper-connection, cyber-harassment, misinformation. Are examples of dangers to which children may be exposed. This is why it is very important to support children and adolescents in their use of the Internet, to ensure their safety and give priority to their physical and mental well-being.

The use of the internet in the educational framework must be able to take place in optimal conditions for students and teachers, in particular by ensuring the protection of minors from an offensive or inappropriate content, or by providing them the necessary culture to protect their personal data

Measures have to be implemented in schools to train and inform users and to set up screening mechanisms:

Schools have to develop a charter for the use of digital and internet. This charter have to be annexed to the internal rules and signed by the students and their parents.

Put in place technical filtering devices: each school have to be equipped with a filtering device of the sites consulted on the internet to allow teaching teams to work calmly and ensure protection of students in case of an inappropriate content.

Other guidelines for schools to monitor online activity of students are:

- 1. Establish a set of rules for using mobile devices or computers during classes display it in the classroom.
- 2. Advice students about how to use the internet safely: do not offer personal information, respect others on the Internet, take care of their accounts with secure passwords, block and report a person who harasses, offends, threatens, limit online socializing.
- 3. Monitoring software.
- 4. Using internet just for educational purpose.
- 5. Teaching students how to react in cases of online violence/ how to deal with harmful content, harmful contact.
- 6. Teaching parents to use apps to monitor control/ the children's online activity.
- 7. Teach online security: strong passwords.
- 8. Recycling programs.
- 9. Recommend sites that provide information, advice and assistance to students, parents about apps and services, how to deal with harmful content or harmful contact.
- 10. Get the parents involved! Organize periodic meetings regarding the phenomenon of cyberbullying and ask them to quickly report any incidents.
- 11. Periodically check security solutions of the computer network in the school. Do not let the students unsupervised in the computer lab.
- 12. Creating an online platform for reporting bullying incidents. <a href="http://brep21.eu">http://brep21.eu</a>



In Romania, the "Save the Children" organization has created a free online safety program and a non-stop telephone line for psychological counselling: Internet Helpline 031 80 80 000.

Our students can also use the website:  $\underline{\text{http://www.oradenet.ro}}$  and the social media:  $\underline{\text{https://www.facebook.com/SigurPeNet}}$ 

The students from all countries can use the site <a href="https://socialmediahelpline.com/">https://socialmediahelpline.com/</a>

They provide direct help advice and information about apps and services, as well as referrals to specialized traditional hotlines and emergency responders where appropriate.

We recommend that you use the site <a href="https://www.betterinternetforkids.eu/sic">https://www.betterinternetforkids.eu/sic</a>

Within the European network of Safer Internet Centres, helplines provide information, advice and assistance to children, young people and parents on how to deal with harmful content, harmful contact, cyberbullying.

# Workshop with parents. How do parents monitor the children's activity online?



The safe and responsible use of the Internet by children depends on the degree of involvement of the parents, on how they establish a dialogue regarding the difficulties on the Internet.

A measure for protecting children while using the Internet and controlling their activity is web content filtering and parental control programs. These are complex programs for controlling children's access to the computer or the Internet, in order to reduce online risks. These programs can be installed on the children's computer or on mobile devices (phone, tablet, iPad, etc.).

It is especially recommended to set separate profiles (users) for children and use these programs when parents cannot be near the children while they are using the Internet.

The main functions of these software solutions are (both for phones and mobile devices and computers):

- block access to certain sites based on a predefined list;
- limit the time spent by children on the computer and/or the Internet, by establishing time intervals in which the child can have access to them;
  - block access to personal or work information stored on the computer;
  - limit or block the use of some programs by children;
  - limit or block access to computer settings;
  - prepare reports with pages visited, programs used;
  - send periodic reports on the children's activity on the computer to the parents' email.

## **How to protect your child from cyberbullying:**

- 1. Be understanding. Don't criticize your child when you realize that what he or she is doing online is inappropriate. Talk to him, ask what websites he is interested in, ask the child to show you his profile on social networking sites.
  - 2. Don't create a fake account and don't impersonate your child's friends.
  - 3. Also warn them not to give out their online passwords to strangers or friends.
  - 4. Explain how important it is for your child to log out of computers they use outside the home.
- 5. Teach them to verify information on the Internet. Remind you that not everything you find online is true.

,,,,,,,,,	as due.
	SAFE CHILDHOOD ONLINE
	Questionnaire for parents
8	Your child has a computer
	• in the room
	• uses the computer of parents/brothers/neighbors/friends
9	How much time does your child spend on the Internet?
	• every day how many hours
	• only when looking for school information
	• when he is alone at home
	• when he goes to friends because we don't have internet
	• Other situations
1	. Which pages/sites do they access frequently?
••••	
1	. Do you help your child to look for information on the Internet that he needs at school to enrich
	his knowledge or to create portfolios?
	• No
	• Sometimes
	• Only if they ask for help
	•Yes
1	. Does your child have a Facebook page?
	• Yes
	• No
1	. Have you seen this page? Do you know what it contains?
	• Yes
	• No
	• Other situation
1	. How does the Internet influence your child's school results?
1	. If your child is fond of computer games, have you noticed if they have influenced hi
	behaviour?
	• manifestations of physical/verbal violence
	• is addicted
	• he no longer leaves the house to play with his friends
	• gets upset when we don't allow him to use the computer
	• without negative influences
	• Other situations

the child's physical health and on intellectual development and communication/socialization possibilities:

16. Write some positive/negative consequences that you think the computer/internet has both on

Content filtering programs web and parental control are programs complexes for controlling children's access and are found for a fee or free of charge and can be installed either on children's computer, either on mobile devices (phone, tablet, iPad). It is recommended especially setting profiles (users) separate for children and their use programs when parents can't be in permanence near children in time what they use the Internet. The main functions of these software solutions are:

- Filtering web content based on restricted address lists or words:
- -blocks access to certain sites based on a predefined list of addresses prohibited.
- allows access only to certain sites

. . . . . . . . .

- based on a predefined list of accepted addresses
- Internet use and access control and computer / mobile devices at programs and files:
- limits children's time to computer and / or Internet, by establishing time intervals in which the child may had access to them;
  - limits program types and files which can be downloaded and installed on computer;
- blocks access to personal information or working stored on computer (for examples, documents, personal photos) by blocking access to certain files or disk partitions
- limits or blocks the use of programs by children (messenger, file sharing, programs used by to parents)
  - limits or blocks access to settings computer
  - Monitoring the use of the computer / mobile device and the Internet:
  - draws up the list of sites that the child has accessed, so that it can be verified by the parents.
- prepares reports with visited pages, programs used, allotted time, files accessed/created/deleted or even images print screen type with children's activity at computer or Internet.
  - send reports by email to parent's periodicals with children's activity at computer.

System configuration Parental control

The parental control system is installed with the Windows7 operating system and you can access it from Start à Control Panel.

Configuring the parental control system is done in a few simple steps. So:

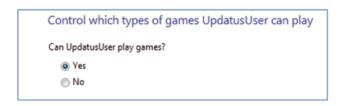
1. Creating user accounts for each child. The main account must be necessarily administered by parents and password protected. For each child in the party must be created a standard user account (Create a new user account à Enter name for new account and press Create account)



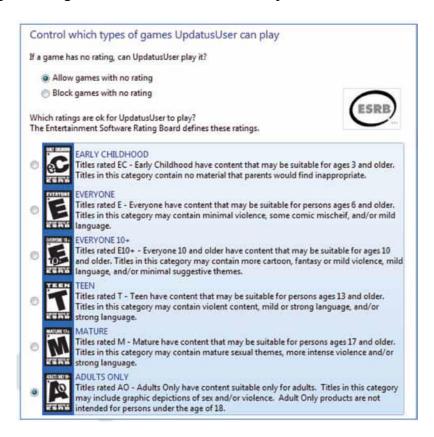
2. The Parental Control System must be opened by selecting the radio button "On, enforce current settings" to start activating the settings in the window below.



- a) Time limits By pressing the "Off" link next to the text "Time limits", a window will open, which allows the program setting to function for that account within a week. Thus, the coloured areas in blue are blocked hours, during to which the account holder does not have access to the computer.
  - b) b. Games (Games) the opening window offers 3 options:
- -Total blocking of access for young people to games by checking the "Yes" button at question: "Can we name user play games?" (Can the X user play games?)



- It is possible to allow access to games depending on the rating system set. Click on link "Set game ratings" and the window below will open:



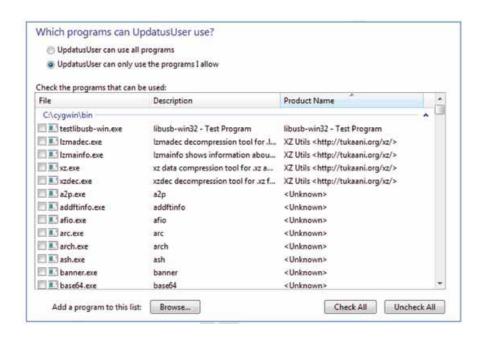
It is also possible to block access to games that do not have a rating system by clicking on the "Block games with no rating" (Locks games without rating system). Then the right rating system can be checked for the child who will use the profile.

Games can also be filtered by type of content, by checking the displayed options following the page. Thus, even if a game respects the rating system but contains images and scenes from the checked list, it will not be able to be played on this profile.

- Blocking certain games – can make a list of blocked or allowed games among those that are installed.



c. Allowing only certain programs – The profile user will only be able to access the programs specified in the list. Click on the "Program limits" link and a window will open as the one below:



Check the allowed programs, and those that want to be blocked are left unchecked.

Safe and responsible use of the Internet by children depends to a large extent measure of parental involvement, how they communicate openly with them about difficulties encountered on the Internet. Children need, first of all, guidance and confirmation from parents' side that their online activities are safe and useful in their education.

#### Conclusions

In conclusion, the advantages of using the internet in education are a testament to its transformative power. As we navigate this educational odyssey, let us embrace the internet as a catalyst for change, fostering a generation of learners equipped with the skills, knowledge, and global awareness necessary to thrive in an interconnected world. The internet, with its vast potential, has become an indispensable tool in shaping the future of education and unlocking the full spectrum of human potential. Each social media platform offers many different ways to be used in the classroom, from sharing announcements to holding live lectures, and so much more. Social media allows for more e-learning opportunities as well.

The negative effects of cyberbullying can be devastating and unfortunately, can affect the emotional and social development of children throughout their lives. Parents, teachers and other authorities must join forces to create a healthy and safe environment for children. Only through education, empathy and the adoption of effective measures can cyberbullying be prevented and combated.

In order to avoid these dangers, parents are advised to bring into the child's daily life activities as engaging as possible, attractive, activities in free time, so that the time spent in the online environment is reduced as much as possible.

The activity in the online environment must be monitored carefully to avoid dangers that can produce negative emotional and physical effects. A measure for protecting children while using the Internet and controlling their activity is web content filtering and parental control programs.

Cyberbullying can affect us in many ways, but the situation can be overcome and confidence and health can be regained. In conclusion, cyberbullying is a type of aggression that has a multitude of long-term negative effects and requires a joint effort of all those involved in the educational process of teenagers.

## **Bibliographique ressources:**

- 1. George Roman, Ghidul utilizării în siguranță a internetului, București, 2014.
- 2. Louie Stowell, Internet en toute sécurité, Usborne, 2017.
- 3. Marius Toma, Cum să utilizăm internetul?, 2002.
- 4. Xavier Tannier, Se protéger sur Internet, Conseils pour la vie en ligne, Eyrolles, 2010.
- 5. https://www.broadbandsearch.net/blog/cyber-bullying-statistics
- 6. https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2019.pdf
- $7.\ http://www.116111.ro/explore/cyberbullying/tipuri-de-cyberbullying$
- 8. https://kidshealth.org/en/parents/cyberbullying.html
- 9. https://techjury.net/stats-about/cyberbullying/
- 10. https://www.wikihow.com/Be-Safe-on-the-Internet