**STRATEGIC PARTNERSHIP BETWEEN SCHOOLS
KA2 ACTION, ERASMUS+ PROGRAM
THE VIRTUAL UNIVERSE WE WANT
PROJECT NO: 2016-1-RO01-KA219-024515**

ROMANIA

GUIDE
FOR PARENTS

STRATEGIC PARTNERSHIP BETWEEN SCHOOLS

KA2 ACTION, ERASMUS+ PROGRAM

THE VIRTUAL UNIVERSE WE WANT

PROJECT NO: 2016-1-RO01-KA219-024515

GUIDE

FOR PARENTS

Tips for parents of the third millennium

Almost 90% of children access the Internet daily or almost daily: in the case of a regular school day, the average time spent on the Internet varies between two to three hours, increasing to over four hours on a free day, showing different studies. In this context, dear responsible parents, how can we control the behavior of our children on the Internet?

---

1. Discover the Internet with your child.

Be the initiators of the child using your computer and mobile phone. The child should know he can talk to his parents about any subject. The positive aspects of the Internet outweigh the negative aspects, so openly communicate to children the advantages and disadvantages of the virtual world.

---

2. Establish with your children rules for using your computer and mobile phone.

Obtaining consensus often leads to responsible behavior on the part of children. There are some sensitive issues that you should agree on, such as types of sites and family activities as well as prohibited ones, or the length of time spent by children on the computer and on the Internet. Personal data rules (family name, age, phone number, photos, address, school, children's place of work, details of credit cards) are essential. Children should also be trained on the programs installed to prevent computer data from being corrupted or lost. Discuss and set up rules about the behavior you have adopted against strangers in the virtual environment (chat, email, SMS, etc.).

---

3. Do not overdo and unreasonably restrict access to the computer and the Internet.

The child will be tempted to hide the Internet's concerns from family members.

---

4. Place your computer in the most accessible room.

For example, in the living or dining room, you can more easily track the sites the child is visiting. Avoid as much as possible letting your child navigate unattended on the Internet in the privacy of his room.

5. Discuss the risks to which they may expose if they accept meetings with unknown people they communicated with by email, chat or mobile phone.

Data on the identity of unknown people (name, gender, age) are often false, in order to be easier to get into a group of children or young people.

6. Make sure you know your child's e-mail passwords or personalized webpages.

So you can find out in advance if malicious persons are trying to get in touch with him. In the case of adolescents, the recommendation is to proceed with care, and they can always change these passwords or create new email addresses. The non-disclosure of the password can also be considered as an act of responsibility on the part of the teenager, meant to provide him with a degree of autonomy. Do not forget to remind them that there are risks to which they can expose and that in any difficult situation they will find you will be ready to help them.

7. Try to learn more about the virtual friends of the children, as you want to know the real world.

Encourage children to tell you about their virtual friends, where they met or discuss. Suddenly shutting down your computer or changing windows quickly on the monitor may be signs of talking to people you should not communicate with.

8. Remind the children that not everything I read or see on the Internet is true.

Suggest to children and other sources of information (books, magazines) and encourage them to create their own opinions on what is true or false. Today, creating a web page or posting information is simple, easy-to-use. In this way, much of the information is unverified, with the risk of being erroneous. Similarly, photos and movies can be easily edited on the computer with powerful software and can portray unreal situations. In other words, not everything flying on the Internet is eaten.

9. Share your experience with other parents.

Concerns you face may find a solution through solutions that other parents already successfully apply.

---

10. To make children safer surfing the Internet, use specialized filtering programs or use your favorite search engine filters.

- Teach the child not to respond to spam emails, harassing messages with offensive, aggressive or obscene content.
- Report any form of abuse to the authorities.
- A complete solution for protecting children while using the Internet and controlling their work on the computer or on mobile and Internet devices is web content filtering and parental control. Web content filtering and parental control programs are complex programs for controlling children's access to your computer or the Internet. These programs are either free of charge or free of charge and can be installed either on your children's computer or on your mobile device (phone, tablet). Parental Filtering and Control Programs are the basic solution to block children from accessing certain sites that may have illegal or harmful content. The main functions of these software solutions, both for phones and mobile devices, and computers, are: filtering web content based on address lists or restricted words; control of Internet surfing through a time schedule established by parents; controlling Internet and computer / mobile access to programs and files, as well as monitoring the use of your computer / mobile device and the Internet.

So take care of your children in the virtual environment, just as you do in real life!

---

11. Communicate openly to children the advantages and disadvantages of the Internet.

---

12. Establish with them a list of safe sites and a computer program.

---

13. The child should know he can talk to parents about any subject.

A solution for protecting the child while using the Internet and controlling his or her activity on the computer or on mobile and internet devices is web content filtering and parental control.

---

14. Teach your children the first rule of Internet navigation - to remain as anonymous as possible.

This means not disclosing personal information (full name, address, telephone number, CNP, passwords, family members, credit card numbers) or posting photos. Personal data and pictures posted in the virtual environment may be used against them.

---

15. Discuss the risks to which they may expose if they accept meetings with unknown people they communicated with by e-mail, chat or mobile phone.

---

16. Try to learn more about children's "online friends", just as you want to know the real world.

---

17. Familiarize yourself with technology and what tools you can use.

Technology is evolving, and we must learn to keep up with it. Our children belong to the generation of "digital natives" and have no problem in using it.

You must understand that technology is your best friend. Use online tools to make sure your little one is safe when using your computer.

However, if you are a busy parent, there are a number of tools that can ease your work and give you a complete picture of what your child does online.

Here are 7 tools to help you make sure you have control:

- Net Nanny – filters content on the internet, blocks pornographic content, timers computer time, monitors social media profiles, and has an alert system alerting you to a threat.
- PureSight PC – protection against cyber bullying on Facebook, pornographic content filtering, online games and activities for parents and children, computer timing system online and offline.
- K9 Web Protection – is a free filter that lets you set and customize your Internet browsing options (you can block some websites that you consider to be harmful).
- Family Cyber Alert – monitors what children do on the computer, online, and on chat platforms through keyboard entries, mouse clicks, and browser activity.

- Anti-Porn Parental Controls – filter that blocks pornographic sites.
- Google Alerts – a free tool that helps you monitor what appears on the internet on certain keywords (for example, your child's name).
- My Mobile Watchdog – app that monitors activity on your mobile phone, from messages, calls, location, installed apps, and time spent on your smartphone.

If you familiarize yourself with the jargon your child uses in his conversations, it will be much easier to understand what you monitor from his online activity.

18. No Facebook up to 13 years old!

Despite the fact that 13 years is the minimum age at which you can create a Facebook profile, over half of parents of 12-year-olds said in a study that they already have an account. Three quarters of parents helped children to do this by their own hands. 30% of parents have admitted to Parenting.com that although they know the rule, they let the children create their account regardless of the restrictions. Although this can not be controlled, you have to respect it if you do not want to end up in extreme situations (see Jezebel Day).

Facebook is the most popular social network in Romania. This does not allow children under the age of 13 to be registered on the platform, but this can not be controlled. Over 20,000 children under the age of 13 try daily to create a Facebook account, registering with a fake, higher age.

19. Monitor and control your child's online activity!
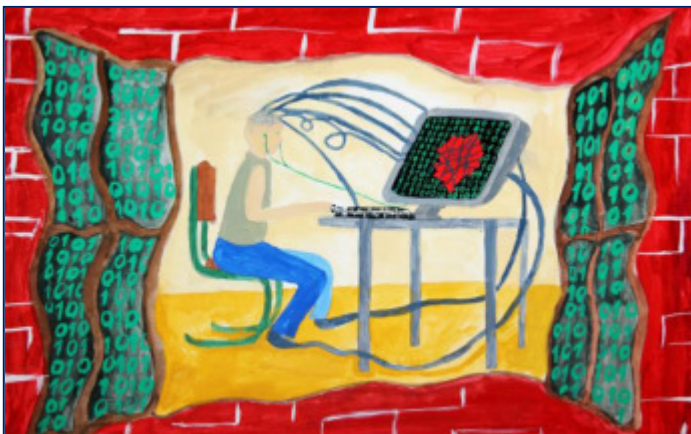
Pay attention to everything: from accounts on social networks to applications on mobile devices. Make sure you keep in mind all the devices you log on, because many of them have dedicated applications and it's important to get rid of anything out of sight.

Here's what you need to do for monitoring and control:

- Make sure you have passwords from all accounts on social networks and chat apps that you can check periodically.
- Check the privacy settings in your browser and make sure they are well restricted.

- install parental control programs (of the previously recommended ones) to track your child's online activity, which sites they visit and what they are looking for.
- Position your computer or laptop somewhere in sight (in the kitchen or dining room), where it will be harder to hide things that you are not allowed to do on the Internet.
- restrict hours of use of your computer and phone (most parental control tools allow you to do this).

20. Avoid apps that do not keep a conversation history!

You have to make sure that it does not use applications that are not indicated to children, such as Snapchat, Wechat, KLIK and Groupme. These applications do not keep a conversation history, so if something bad happens, you will not find the traces of the facts and you will not be able to act properly.

21. Teach him about responsible use of the internet!

The child should be educated to behave in the online environment just as it would in real life. He must learn about the online reputation and the risks he is exposed to, but in particular he must know how to act in crisis situations.

22. Show him he can trust you!

This is the most important thing. The child must know that he can rely on you in any situation. He must understand that whatever happens, he can turn to you without being afraid or ashamed.

Are these measures exaggerated?

Bibliography:

http://www.darabaneni.ro/social/au-navigheaza-pe-internet-vezi-sfaturile-oamenilor-legii-pe/

www.sigur.info/siguranta-online/copii-pe-internet/copii.html

www.salvaticopiii.ro/.../p0001000100010000_Ghid%20SigurInfo%20165x235%20re..

List of illustrations- art works created by the students of „Bălaşa Doamna" Art High School- Târgovişte

Pg. 1 Alina Baciu -10th grade
Pg. 2 Ştefan Grigorescu -11th grade
Pg. 4 Maria Netbai -11th grade
Pg. 5 Bianca Cernat -11th grade
Pg. 6 Florinel Moiceanu -11th grade

GUIDE
FOR STUDENTS

STRATEGIC PARTNERSHIP BETWEEN SCHOOLS

KA2 ACTION, ERASMUS+ PROGRAM

THE VIRTUAL UNIVERSE WE WANT

PROJECT NO: 2016-1-RO01-KA219-024515

GUIDE

FOR STUDENTS

Guide for students

What is Cyberbullying?

Internet aggression, also known as **online bullying** or **cyberbullying,** is bullying by computer or cell phone. Bullying takes place on blogs, personal pages, forums, e-mail, SMS, MMS, sometimes aggression by uploading pictures or video on the Internet without taking into account the victim's privacy.

By cyberbullying is meant to offend, threaten, mock and humiliate others with premeditation by means of modern means of communication - usually for a long time.

This type of bullying takes place on the Internet (for example via emails, Messenger, social networks or via video on specific portals), on the mobile phone (for example via messages / SMS or repeated upsetting calls). The perpetrator - also called bully - usually acts anonymously so that the victim does not know who is behind the attacks.

When it comes to bullying children or young people in virtual space, victims and perpetrators are often known in real life. As a rule, victims already assume who the aggressors are. This type of bullying comes from the environment of the students - the school, the neighborhood, the village or the ethnic community to which the victims belong. The cases in which a stranger was the perpetrator are very rare.

About Cyberbullying

Internet bullying has already reached alarming levels, and victims of the phenomenon do not have many weapons available to protect themselves from this. Physical appearance, passions and material status are among the main reasons. The main weapons of attack used on the Internet to assault victims are linked to the appearance and the way they dress. Other common reasons why young people are bully are daily hobbies and concerns, the material situation of their family, school results, and sexual orientation.

Two-thirds of those who are bully did not tell anyone about the incident, with young people citing reasons such as fear, lack of confidence that they might change something, or the

fact that they did not think it necessary to involve other people even though they were directly affected by aggression.

The most popular social networks where cyberbullying takes place are Facebook, Messenger, and Instagram, and the means of propagating the most commonly used phenomenon are threatening and negative messages received in the private channel followed by negative comments photos and identity theft. Most say that incidents of this kind have lowered their self-confidence and have led them to isolate themselves. Few, but not neglected, are those who have said they have entered depression or compensated for the lack of online friends by drinking alcohol or drugs. Moreover, many say they have witnessed such an attack without being aggressors or victims, but only a few have intervened in the conflict between the two sides. Although most would have liked to take the part of the bullying, most become indifferent or even aggressor for fear of being attacked and turning into victims.

Adults, teachers, parents or any other person to whom an abused person feels attached must provide unconditional and trustworthy support. The victim has to report any action that has taken place on him, but he needs extremely trusted allies to provide the comfort of talking.

Parents, teachers need to be aware of the phenomenon and know how to identify the victim's changed behavior and intervene when identifying the effects of cyberbulling in its behavior. Any sign indicating changes in psychological status such as depression, social anxiety, isolation, low self-appreciation, negative reactions, and stress with regard to the use of electronic devices must be questioned and verified. It is useful for the victim to succeed in imposing limits. From blocking and reporting the abuser on social networks, changing passwords or phone numbers to direct abuser interventions, done in a more assertive manner, without offering the aggressor the satisfaction they are looking for. The harrased person will be pleased if he / she causes the victim to suffer, so it is recommended to avoid showing any trace that indicates that it has been affected.

The intimidation can be:

- **Verbal -** nicknaming, insult, offense, threats, sarcastic replies, inappropriate sexual comments, offensive replies, defamation etc.
- **Social -** incitement to hate, deliberate exclusion of someone from a group, diffusion rumors, public humiliation, defamation or damage to reputation in order to isolate.
- **Physics -** hitting, kneading, spitting, personal damage, etc.
- **Online -** malicious texts or emails with negative messages, widespread rumors, or ironing a person through e-mail or social networking sites, distributing offending pictures or videos, creating false profiles, etc.

Being terrorize can happen to anyone, anytime. You are the victim of online bullying if you find yourself in at least one of the following statements:

- your personal space or home has been invaded electronically. It can be done virtually by any means, from text and visual messages sent by e-mail or SMS to aggressive posts or rumors spread on blogs and social networks;
- offensive messages about you are displayed in public space;
- you have created one or more false profiles;
- web pages have been created with information about you and trying to intimidate you.
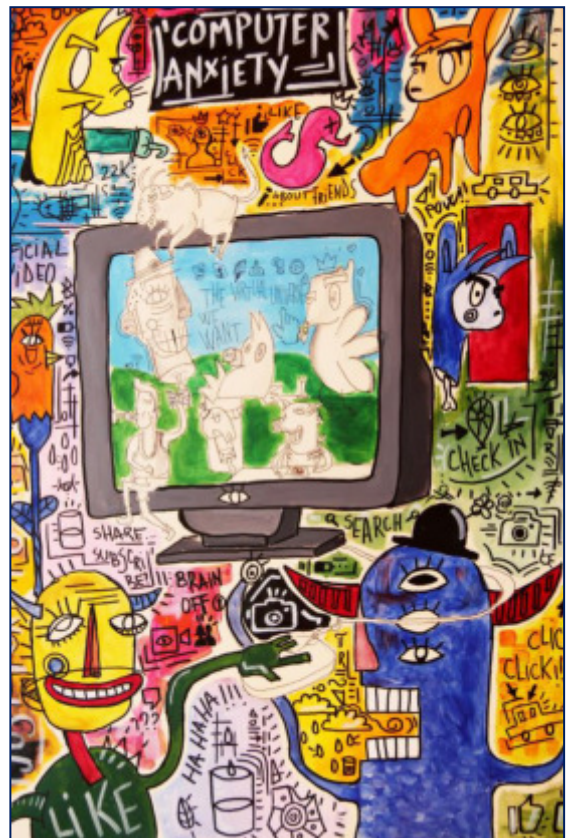
Online bullying

Online bullying is a complex phenomenon that takes place in the virtual environment with the help of electronic communication technologies and services. What makes online bullying even more dangerous is that once the disturbing information about you is posted on the Internet, it's very hard to eliminate it permanently because someone else might copy and post them elsewhere, and the rhythm of multiplying those posts is even greater than in real life.

Online bullying modes:

- **The aggressor is the victim of bullying**

Online aggression can begin with the fact that the aggressor is a victim. By illegally accessing the victim's account (accessing the account can only take place if the abuser knows the password), the abuser sends injured messages to those on the victim's contact list, creating problems between the victim and the victim. Then changing the password, the aggressor prevents the victim from entering his account (Facebook). Another method used by the aggressor is to open an account on behalf of the victim and to use it by claiming to be the victim. Keeping your password secret even for your closest friends is therefore absolutely necessary.

- **Aggression on web sites**

Aggression can take place through different methods:

Hateful sites: The aggressor creates a "hate site" to terrorize an individual. This may mean posting pictures or videos that show the victim in embarrassing situations. Or sites that vote for who is the most ugliest, etc.

Hate groups: Such groups sometimes appear on Facebook or other social networks. The groups share the fact that I hate a whole group of people. Even if the site administrator cancels the account, the attacker opens another account that continues aggression.

- **Mobile phone aggression**

The most commonly used method is to send messages with offensive content. Content can be verbal or images.

- **Aggression on blogs**

The aggressor writes comments with injurious content to the victim.

- **Aggression through voting on the Internet**

Who is the most beautiful or the most ugly? Such questions are examples of online aggression.

Rules of conduct to prevent cyberbulling

The Internet is a fantastic world full of useful information and fun things to which all children are entitled. But this world also hides danger that can be avoided if you follow the following rules:

- **Establish with your parents the rules for using the computer and the Internet.**

You can make a list of the websites you want to browse or suggest your parents and decide by mutual agreement the times when it is best to use the Internet. Your computer can help you do your homework or spend your time in a pleasant way. Parents can teach you how to find useful information faster, but you can also show how good you are in using your computer.

- **Do not give any person on the Internet personal information about yourself or your family.**

These may be the name, age, phone number, photos, address, school you are studying, parents' place of work, etc. When these strangers insist (by email, chat or cell phone) to find out who you are and where you live, tell your parents immediately.

- **Passwords are secret and you belong.**

They are like the keys to the house that you do not give to anyone, even the acquaintances. Except for parents! You must always reject friends who ask for your password because they can use your email address to send offensive messages to other people or to enter forbidden sites. If you suspect that your password has been disclosed, change it immediately, alone or with the help of your parents.

- **If you want to meet face to face with people known on the Internet or from whom you have received messages on your mobile phone, tell your parents to go with you, preferably in a public place.**

Never accept to go alone. People can be very different from what they seem to be on the Internet. Not a few times the boys turn out to be girls or vice versa, or the stated age is not the real one. To avoid any danger, do not use your personal phone to call someone on the Internet. Talk to your parents first.

- **Carefully post photos with you or your family!**

When you want to upload photos or movies to sites you need to create a profile or account (such as Hi5, My Space etc.), select the files with your parents. Learn to create a list of people who can see your profile. Use webcam only when your parents are with you. Remember, photos or videos, once posted, can stay forever on the Internet even if you delete them!

- **Not everything you read or see on the Internet is true.**

  Today, many people, including children, can create web pages or post texts, photos, news. In addition, photos and movies can be easily edited on your computer. To check if what you found on the Internet is true, ask for help from your parents or teachers who can provide you with other sources of information. Do not download or install pirate programs or do not know them, they can destroy data on your computer.

- **Do not respond to messages that upset you or contain inappropriate words or images!**

  Keep them to show their parents, teachers or, in serious cases, the police. If you receive emails, files, photos or installation programs that seem suspicious of someone you do not know and trust, delete them from your computer. They may have viruses or programs that will read all the data on your computer. Ask for help from a trusted person.

- **It shows respect, even if you do not know the people you communicate with.**

  Your duty is to protect others too. It does not send offensive images or messages that may cause fear .

- **Buying products on the Internet is only allowed for parents.**

  They are the only ones who are allowed to use credit cards. So tell your parents whenever they were sent to you by e-mail or chat, offers or requests for money.

- **You can always stop surfing the Internet or refuse to continue chatting if something happened that you did not like, scared you or just did not understand.**

  Talk directly to your parents or teachers and explain what has worried you. You can always remove contacts you do not want to communicate with.
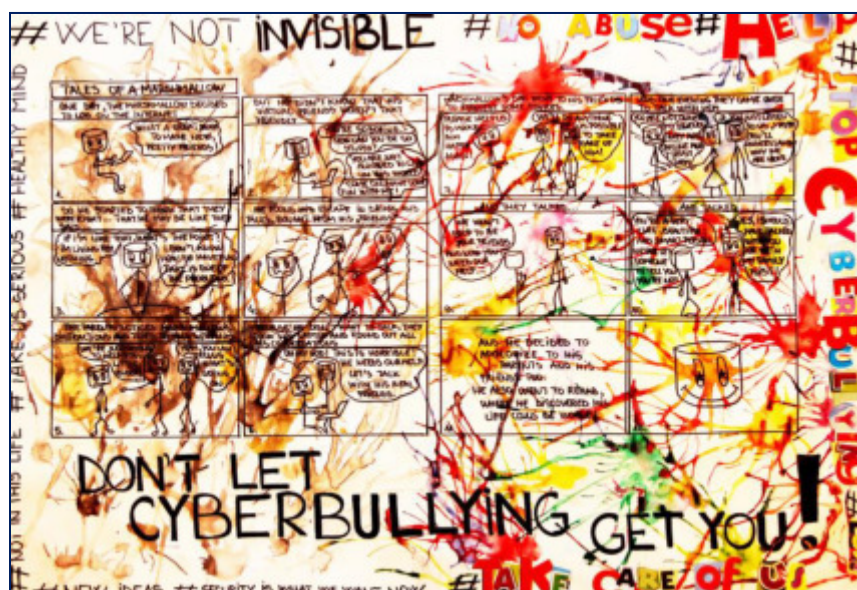
The Norwegian site Barnevakten.no recommends 10 online behavior rules:

1. Be honest and polite!
2. Think about what you are writing!
3. It respects people of different ethnicity or race and those who have another way of life!
4. He respects the law of his own country and the law of the country where the correspondent is!
5. Respect copyright, whether it's text, images, sound or software!
6. It does not send pornographic material with violent, racist or blasphemous content!
7. Respect other users!
8. Be smart in spending money online!
9. Report the illegalities you see!
10. Do not forget that other children are also using forums!
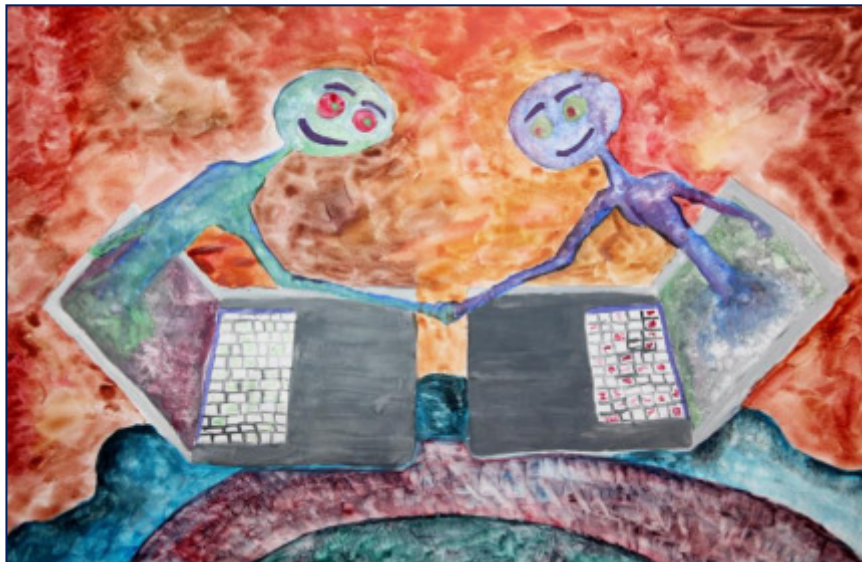
Legal remedies

Cyberbullying becomes a growing problem every day. Every day, thousands of people have to deal with negative, abusive, offensive and threatening posts, messages or comments. This has led to the following question: What legal solutions do I have to protect myself from Internet bullying?

Abuse on social networks.

Suppose abuse occurs on a social network like Facebook, Instagram, Twitter, etc. The first step is to notify the site, as most social networks now offer users the ability to report spam, abusive comments, or bullying. Reporting multiple or multiple people to a person's abusive

behavior on the Internet may result in the closure of that account or even prohibiting that IP from accessing it for the future.

Abuse outside social networks.

If the abuse occurs on a particular website outside the social network, such as a defamatory article for a person, the first step is to notify the owner of that site about the deletion of the offending content. Since most sites do not want to be trapped in the dispute between the two parties, in order to avoid lawsuits or other legal consequences, they will usually delete the offending material.

Referral to criminal authorities

Unfortunately, however, it is not always possible to solve the problem without resorting to criminal organs. There may be situations where the site does not intervene or fails to take effective action to stop the bullying, or the user resorts to threats or blackmail that affect the victim's freedom and safety and a simple deletion of the content is not sufficient to protect the victim.

In this case, the legal remedy is the filing of a criminal complaint for the offending offenses, such as the threat (Article 206 of the Criminal Code), blackmail (Article 207 of the Criminal Code) and / or bullying (Article 209 of the Criminal Code).

Summoning the aggressor

If the first two solutions did not work, either the site failed to stop the abuse, or it was considered that the act was not a crime and the case file was ordered, the only remaining solution is the opening of a civil litigation.

Article 72 of the Civil Code provides that *"(1) Everyone has the right to respect for his dignity. (2) Any harm to the honor and reputation of a person is prohibited without its consent."*

Article 73 of the Civil Code provides that *"(1) Everyone has the right to his own image. 2. In the exercise of the right to its own image, it may prohibit or impede the reproduction in any way of its physical appearance or voice or, where appropriate, the use of such reproduction.*"

The first step is to file a lawsuit against the side on the basis of tort law, by which you may request:

- Remove related content as it affects your image, honor and reputation, under art. 73 of the Civil Code.
- Civil liability for the damage caused, namely obtaining material and moral damages.

The new Civil Code enshrines, in principle, **the full reparation of the damage.** So, you will be able to claim and obtain both material damages and moral damages as a result of touching your image, your reputation for freedom and security, to compensate for the loss suffered as a result of that unlawful act.

Bibliography:

http://adevarul.ro/tech/internet/hartuirea-online-cyberbullying-ul-cele-mai-mari-probleme-internet-adolescenti-afectati-1_5a1bf67f5ab6550cb895be91/index.html

https://ro.wikipedia.org/wiki/Agresiunea_pe_Internet

http://www.totuldespremame.ro/copilul-tau/psihologie-si-comportament/dusmanii-de-dincolo-de-ecran-bullying-ul-virtual-sau-cyberbullying-ul

https://oradenet.salvaticopiii.ro/viata-ta-online/prietenii/ce-este-cyberbullying-ul

http://cyberhelp.eu/ro/introduction/what_is

https://www.bitdefender.ro/news/80-dintre-adolescenti-au-fost-hartuiti-pe-internet-aspectul-fizic-pasiunile-si-situatia-materiala-principalele-motive-3393.html

List of illustrations- art works created by the students of „Bălaşa Doamna" Art High School- Târgovişte

Pg. 2 Ştefania Duţă, Iulia Gălbenuş, Elena Tudose -10th grade
Pg. 3 Teodora Mihăilă -12th grade
Pg. 4 Florinel Moiceanu -11th grade
Pg. 5 Maria Netbai -11th grade
Pg. 6 Andreea Iacob -10th grade
Pg. 7 Ştefan Grogorescu -11th grade
Pg. 8 Ioana Alecu -11th grade

GUIDE
FOR TEACHERS

STRATEGIC PARTNERSHIP BETWEEN SCHOOLS

KA2 ACTION, ERASMUS+ PROGRAM

THE VIRTUAL UNIVERSE WE WANT

PROJECT NO: 2016-1-RO01-KA219-024515

GUIDE

FOR TEACHERS

CYBERBULLYING INTERVENTION GUIDE FOR TEACHERS

HOW DOES SCHOOL GET INVOLVED IN CASES OF VIRTUAL AGGRESSION

For such situations, school should develop and implement response procedures in case of suspected or confirmed suspicion of a child's involvement in a potentially dangerous online event. Written and distributed procedures for school staff should clearly inform on the practical ways in which teachers need to identify and behave in relation to potential victims of online threats and, as the case may be, manage the relationships with the involved parties: potential authors, witnesses and parents.

These procedures can be carried out by school staff, but it is recommended to involve external consultants with online security expertise and tailored to the specific reality of the school.

The procedures must take into account several significant basic elements:

• the prioritization of specific victim support activities, which has often been omitted in the context of efforts to reduce the impact of an online incident;
• to contain concrete action elements that will allow the events documentation and the preservation of eventual evidence;
• concrete ways of involving parents in solving the incident;
• concrete elements of possible cooperation with competent institutions - from specialized psychological assistance to cooperation with law enforcement.

That is why it is necessary to constantly know the potential online threats, together with their specific characterization elements and develop concrete procedures to approach each possible situation.

Cyber-violence (from the English Cyberbullying, a category that includes aggression by electronic means) is any deliberate action involving the use of the Internet, the computer or mobile devices (mobile phones, tablets, etc.) that is intended to cause material or psychological harm to the victim.

Electronic aggression can affect people of all ages, while the term "cyber-violence" is reserved to the aggression where the authors or the victims are children and young people.

Independently of the person reporting a case of cyber-violence, the response procedure should include:

• providing support for the victim of violence;

• preserving the evidence and establishing the circumstances of the action;

• ensuring conditions to attract authors' responsibility for the consequences of their actions;

• providing specific activities to determine the change of attitude of the guilty student towards the committed actions.

All cases of violence, and therefore violence through the use of electronic means, must be looked into / legally investigated, recorded and documented.

1. If the information about the incident has been the subject of informing a teacher other than the homeroom teacher or the teacher responsible for the class in which the aggression was committed, he shall inform the responsible teacher as soon as possible, who shall in turn inform the school headmaster;

2. The school headmaster and, depending on the nature of the incident, the school psychologist, in collaboration with the homeroom teacher, should analyze the events and plan future actions;

3. According to its attributions, the school representatives must also determine the circumstances of the occurrence of the incident and, as far as possible, identify the potential witnesses;

4. In the intervention procedure, the presence of the IT teacher must also be foreseen, in particular during the protection and preservation of evidence stage and the conduct of checks. Any evidence associated with a cyber-violence incident / incident must be preserved and recorded. The registration in any form must contain the date and time of receipt of the material, the content (the text) and, if possible, details of the sender (user name, e-mail address, mobile phone number, etc.) or web site where the incriminating content or profile was found and verified in advance;

5.   Protecting / preserving samples facilitates the activities to be carried out in cooperation with the service providers (requesting data to the Internet service provider or web services for user identification data, deleting offensive content, etc.), being necessary to all parties involved: school leadership, psychologist, homeroom teacher or other entitled teacher, parents and, if there are indications of committing a crime, to law enforcement.

How can you keep / preserve the evidence in a cyber-violence incident?

•   Mobile phone: do not delete the message. Save all text or voicemail messages in your voice mailbox.

• Instant messaging (SMS / MMS). Some services allow recording of conversations. There is, for example, the ability to copy / re-transcribe an oral conversation, and the ability to copy SMS and MMS to a Word document (or other text editor) to save and print them.

•   Social networking sites or any web site / www. To keep a copy of the content displayed on the screen, click Control and Print Screen (use the "Capture" tool on Macintosh), and then paste into a Word document.

• Chat. As well as on the web, if you want to keep a copy of the on-screen content, click Control and Print Screen (use the Capture tool on Macintosh), and then paste it into a Word document, or simply print the desired page.

• E-mail. Copy and print the message, send it to the homeroom teacher or the responsible teacher who will be involved in determining the circumstances of the incident. Save the full message, not just the text, as it will preserve all its origin data.
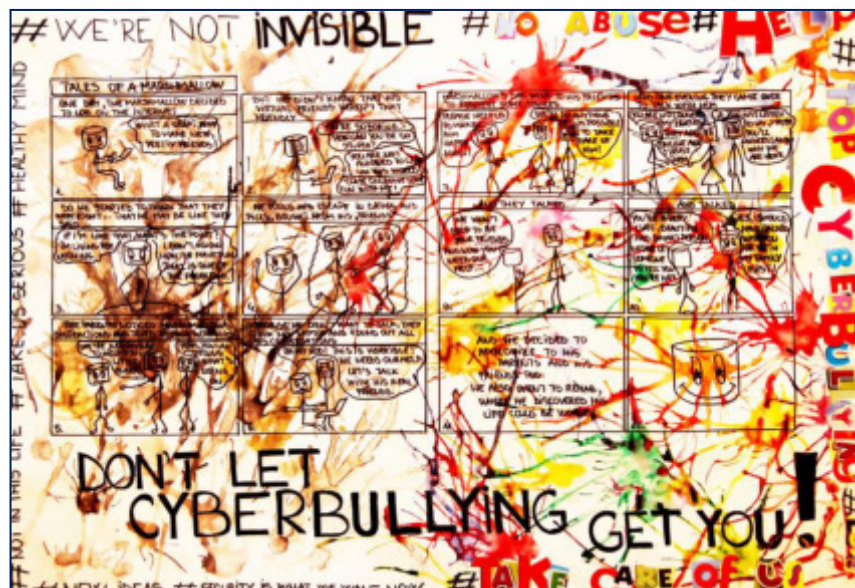
Identifying the author

The persons empowered to check the circumstances of such an incident must have the necessary knowledge to identify the relevant data and must take into account that data extracted from electronic means are not sufficient to track/ identify the author.

1. Many authors of cyber-violence facts use false electronic identities, for example, using other students 'phones, profiles on social networks that do not belong to them, others' email accounts, mail accounts, or accounts created on websites providing false data about their own identity, etc., for the purpose of sending messages or publishing offensive material. Difficulties in tracking or identifying a "cyber aggressor" can also occur when the material is sent through mobile devices connected to open wireless networks, or when anonymization facilities are used by proxy servers, both variants being currently widely available .

1. According to a number of cases, for most of the incidents of this kind, the identification of the aggressor is not very difficult. The victims of cyber-violence are often able to identify the perpetrator of the crime (quite often he / she being a colleague or an entourage).

2. If the author can not be identified, you should contact your service provider to remove compromising / offensive material from the net. Art. 16 of the Law no. 365 of 2002 on electronic commerce establishes rights for persons who may be harmed by the content of some web pages hosted on the territory of Romania and obligations for the providers of such services.

3. If it is established or is obvious that the law has been violated and the identity of the author (s) could not be determined, it is mandatory to contact the police.

How to deal with the perpetrators of violence through electronic means

When the author of the cyber-violence incident is known and is a student of the school, the homeroom teacher /primary level teacher and the school psychologist should perform the following activities:

1. Discussion / conversation with the student responsible for his / her behavior, following the following points:

• determine the circumstances of the incident, in order to identify together the causes and find a solution to settle the conflict;

• the author must receive a firm message that such acts are prohibited without any derogation;

• the student should be informed of the consequences of his / her behavior and of the legal regulations and / or norms to which he / she will be called upon to enforce his / her deed;

• determination of the author to delete any offensive material published online;

• In the discussion, depending on the gravity and nature of the facts, the possibility of mediation between the parties and the identification of possible remedies should be considered;

• if there were several authors, each of them should be discussed with and their leader identified;

• The author should not be confronted with the victim of violence by electronic means.

2. Communicating with the author's parents and discussing their child's behavior:

the parents of the author must be informed of his actions and must be presented with the evidence that led to this conclusion, and on that occasion they are also informed of the disciplinary measures that the school can order against the child.

3. Providing psycho-pedagogical assistance to the author:

• communicating with the author of the incident should help the student understand the consequences of his behavior and seek to change his / her attitude in relation to the facts and the way of using the new technologies;

• if the school has appropriate conditions, specialized psychological assistance can be provided within the school;

• In some duly justified cases, the pupil may be offered a psychological assistance program within a specialized institution during the discussion (with the consent of the parents).

Aspects that can support the author's identification

1. Witnesses - other students who view the offensive content, who may have information about the author, about the potential conflict between the parties or can identify him /her with available data (telephone number, e-mail address, etc.)

2. Contact your web hosting provider involved in the incident (webpage, discussion forum, etc.) or Internet Service Provider (it will analyze the specificity of the incident and the resources used by the author) - thus the author's account can be blocked / suspended, the offensive content can be removed, and additional data about the authors of the violence can be obtained by electronic means, and any law enforcement actions to identify the author can be facilitated (if the situation so requires, legal measures against the services involved can only be arranged in cooperation with the responsible state authorities).

3. Contacting the mobile service provider - if the phone number is hidden, the operator has the ability to identify the calling number, if the called phone number, the date and the time of the call are provided. These data may be transmitted by the operator only to the law enforcement authorities.

4. If possible, parents should also be involved in the attempt to raise the awareness of the student on the effects of violence by electronic means; a commitment involving the parents, the school's representative and the student can be also signed in order to make sure that the student has been informed on the rules of online behaviour, as well as the administrative and legal consequences of non-compliance.

Disciplinary measures for authors of violence by electronic means

1. Violence by electronic means should be sanctioned by the provisions of the school regulation, with consequences similar to acts of physical violence. In addition, specific to these types of deeds, sanctions may be applied such as: prohibiting the access for a limited period of time in the computer lab or the introduction into the school of electronic devices that have connectivity to the Internet or the mobile electronic communication network.

2. The main objectives to be considered in relation to the sanction against the author are:

• immediate cessation of the act of violence and guaranteeing a sense of security for the victim;
• awareness of his/her behavior, of the problems he/she has generated and the prevention of similar behavior in the future;

• to show the school community that cyber-violence will not be tolerated in any way and that the school is able to respond effectively to such situations.

3. In determining the most appropriate sanction, consideration should be given to:
• the size and importance of the damage / effects generated - whether the material has been made public in a way that has allowed access to a wider audience (this determines the extent of the victim's humiliation) or whether it is difficult to remove the offensive material from the Internet, etc
• victim's persecution duration: it was a prolonged exposure or one episode;

• premeditation of the deed - if the deed was planned and if the author was aware that it would create harm to a colleague (some cyber-violence actions are caused by unconsciousness or lack of awareness of the consequences);

• an interesting factor is to see how many efforts the author has filed to hide his identity, etc .;

• the author's motivation. You need to make sure that his/her action is not revengeful, out of a potential persecution previously suffered;

• the type of the distributed offensive material.

Measures to support victims of violence through electronic means

1. Psychological support

As in the case of other forms of violence, the victim of cyber-violence needs help and emotional support from adults.

The victim must also know that the school will take firm action to resolve the issue.

During the conversation with the student who is a victim of cyber-violence, the following steps must be taken:

• ensure him/her he did something right, reporting the incident;

• ensure him/her that you understand the feelings he/she experiences and the fact that it is difficult for him/her to reveal the incident, and strongly advise that no one has the right to treat him/her in this way;

• ensure him/her that the school does not tolerate or support any form of violence and adopts appropriate response measures to the situation;

• pay attention to the non-verbal expressions of the child's feelings - embarrassment, shame, fear, fear, sadness, feeling of guilt.

2. Recommendation

The student who becomes the victim of cyber-violence should be advised how to behave in order to maintain a sense of security and to avoid escalating the feeling of persecution.

Recommendations to follow for the victim:

• do not keep in touch with the author, do not respond to emails, telephone calls or any other means of contact that may be used by him/her;

• do not delete or hide evidence: email, SMS, MMS, photo, video and present them to the school's staff or parents;

• it is recommended to change the phone number, the email address, the accounts used on social networks, etc .;

• if the student is using online messaging services, make sure that he/she can only be contacted by known people (most profile services allow you to set up user lists with whom conversations can be engaged , also allowing to block others).

3. Monitoring

After the initial intervention, the student's progress should be constantly monitored so as to avoid further actions against him, or even acts of revenge with violence or blackmail actions by the author.

The victim's parents need to be informed about the problem and accept the support of the school unit. During a meeting with the homeroom teacher, the primary school teacher, or the psychologist, they must be presented with the measures that have been taken to clarify the incident and guarantee the safety of the student - victim. If necessary, it should be proposed to the parents and child to seek the support of a psychologist specialised in this field.

How to behave with a witness that signals an act of cyber-violence

1. Tell him/her that the report of the act of violence is a correct action.

2. Send it clear that this gesture requires a lot of courage on his part.

3. Ensure him/her of your total discretion.

  Do not disclose its data if it is not necessary (for example, his/her identity can only be revealed when the problem is reported to the police).

  4. Under no circumstances will you confront him/her with the author of the deed.

  5. Take care of him/her and his/her security, do not publicize his/her involvement in the case.

Preparation of incident documentation

1. The educator / psychologist has the obligation to draw up a documentary of the incident, which must contain the documents to support and prove, if necessary, communication with the author, the victim, their parents and the witnesses, as well as any activities / measures in the case. The documents must contain the date and place of the discussions, the participants' personal data and a description of the approach and content of the conversation.

2. If conversations take place in the presence of a witness (eg another teacher), the documents are also signed by the witness.

3. If cyber-violence samples have been preserved and protected, they must be added to the file / record of the incident (description, printed inventory, etc.).

School collaboration with law enforcement authorities

Most cyber-violence cases do not require law enforcement authorities to be informed and can be resolved using the resources available at school level.

However, there are situations in which police need to be notified as follows:

• the parents of the perpetrator of the violence by electronic means refuse to cooperate or do not appear at school at the request of the teaching staff or the student does not abandon the activity that generated the incident. Under these circumstances, school leadership must report in writing to the police the situation in the institution.

• when the school has exhausted all the available educational means (eg meetings with the parents of the authors, the application of the disciplinary measures provided by the school regulations to the author, meetings of the author with the school psychologist, etc.), without achieving the desired results, the school leadership has to notify the competent authorities, according to the legislation in force.

• the school is required to notify law enforcement authorities even the cases of violence by electronic means which have been reported ex officio.

Bibliography:

http://www.securitate-online.ro/wp-content/uploads/2015/10/Standarde_pentru_securitatea_online.pdf

www.sigur.info/siguranta-online/copii-pe-internet/copii.html

www.salvaticopiii.ro/.../p0001000100010000_Ghid%20SigurInfo%20165x235%20re..

List of illustrations- art works created by the students of „Bălaşa Doamna" Art High School- Târgovişte

Pg. 2 Ioana Alecu -11th grade
Pg. 3 Andreea Iacob -10th grade
Pg. 4 Florinel Moiceanu -11th grade
Pg. 5 Teodora Mihăilă -12th grade
Pg. 6 Alexandra Şerbănescu -11th grade
Pg. 7 Ştefania Duţă, Iulia Gălbenuş, Elena Tudose   -10th grade
Pg. 8 Oana Popescu -12th grade
Pg. 9 Bianca Cernat -11th grade
Pg. 11 Ştefan Grigorescu 11th grade