CYBERBULLYING AND PRIVACY

GUIDE FOR TEACHERS

protegeles.com

FINANCIADO POR LA COMISIÓN EUROPEA

daphne

CYBERBULLYING AND PRIVACY

GUIDE FOR TEACHERS

1. RATIONALE FOR THE GUIDE

"European Superkids Online" is a project integrated into the Daphne III Programme, which is financed by the European Commission. Its main goal is to strengthen teenagers against online violence, using e-learning modules. The countries and organizations that have cooperated in this project are Italy (Save the Children Italy), Poland (Nobody´ s Children Foundation), Denmark (Save the Children Denmark) and Spain (PROTEGELES).

There is currently a great international concern about the increase of online violence among teenagers. The widespread use of new technologies has lead to the appearance and expansion of phenomena such as cyberbullying (bullying using new technologies), together with other problems which may also mix with it, such as identity thefts, threats, slanders, insults, etc.

In addition to this problem, other types of conflictive situations also take place in the Internet, which require special attention and handling. Problems such as grooming (sexual harassment using new technologies), sexting (sending images of sexual or exhibitionist content) and, in general, anything related to the lack of privacy in the Internet reveal the need to intervene in order to prevent those risks or to tackle them successfully once they have occurred.

In this Project, each country has customized the topics to be dealt with according to the teenagers' needs previously detected. In SPAIN, PROTÉGELES has carried out a series of surveys and interviews with teenagers. The outcome has revealed that it is necessary to work with them on the topic of cyberbullying, and that it is also key to convey to them how important it is to protect their privacy when they are online.

The e-learning modules have been specifically designed and adapted to teenagers between 10 and 13 years of age. Parents, teachers and educators may use these modules to work with that age group.

Schools are the perfect place to enrich students' experience of the digital world, as well as to train them on how to do a safe and responsible use of ICTs. Teachers and educators have often expressed their need of specific resources and materials to be able to work on these topics in the classroom. This guide aims to be a resource with the necessary information and material to train teenagers and reflect with them about these issues in their school and home environments.

This guide is therefore also available for parents who are actively involved in the IT education of their children. They will also find all the necessary information and resources to talk about this kind of phenomena at home.

This is how the project "European Superkids Online" appeared in the European Union, with the goal of offering the target groups a resource – including theoretical information and hands-on activities (videos, case studies, tests...) – they can use to train and prevent risk behaviour with regards to cyberbullying, and to promote the protection of teenagers' online privacy.

2. INTRODUCTION

We call them "new technologies", but we must bear in mind that for teenagers they are nothing "new": simply tools with which they've grown and that are perfectly well integrated into their lives, their leisure activities and their relationships. Although most adults use ICTs for work-related activities, teenagers use them mainly to communicate with others and for social interactions, as well as to have fun or simply pass the time. They use them increasingly for school-related activities, but this is still the last reason for them to go online.

Furthermore, only computers with an Internet connexion are used to do school work, in opposition to their widespread use of mobile devices, smartphones and so on for other purposes.

Nevertheless, the fact that teenagers frequently use the Internet and new technologies does not imply that they know how to do it safely. It also does not mean they use them in a responsible fashion or knowing the consequences they may suffer if something they do while using the Internet or the new technologies is harmful to others. This inadequate use may expose teenagers to many risks, two of which are highlighted in this guide: the risks derived from the lack of privacy in the Internet, and conflicts that may generate among teenagers and which may end up in the Internet. Through the Internet and in particular through social media, teenagers share all sorts of information: they give their personal details, they upload photographs of themselves and of family and friends, they talk about their likes and preferences, about what they do, their plans and even their feelings and concerns. The kind of things which were only known by their group of friends some years ago, can now be seen by millions of people. Logically, this may lead to risk situations.

Besides, we must bear in mind that currently many conflicts that take place at school end up in the Internet and vice versa. These conflicts may degenerate into systematic bullying through the use of new technologies, which is promoted by the alleged anonymity young people believe they have when they are online. This phenomenon of bullying under several formats is known as cyberbullying. It is clearly a growing problem affecting both direct victims and people around the victims, and which requires the cooperation and involvement of teenagers in order to prevent it and settle it.

All the professionals working with teenagers must commit themselves to conveying the need to use ICTs in a safe and responsible manner. Taking into account that students spend most of their time at school, schools are the perfect place to teach them how to carry out social interactions in a positive way, both online and offline, as well as to take care of their own privacy as well as other people's privacy.

This guide aims to be a useful resource that will make this task easier for teachers, helping them train students how to USE ICTs IN A SAFE AND RESPONSIBLE MANNER by focusing on two main aspects: cyberbullying prevention and the importance of privacy protection in the Internet.

3. CONTENTS OF THE GUIDE

3.1 CYBERBULLYING

3.1.1 WHAT IT IS AND WHO IS INVOLVED

Cyberbullying is a sustained and repeated psychological aggression carried out by one or several users against another user, through information and communication technologies (ICTs). Unlike traditional bullying, cyberbullying may be maintained 24 hours a day, as the aggressor may access electronic devices at any time and from any place, so the damage done to the victim may be significantly greater.

Participants: Victim and harasser/s.

1. Students who attend the same school
2. Students who attend different schools.

It is an action carried out behind the adults' back and which is strengthened by specific situations, such as the following ones:

1) The aggressor or aggressors are not forced to witness the victim's reaction, and this inhibits the mechanisms that could launched by face-to-face empathy.

2) Many Internet users share the false belief that the Internet in some way guarantees the alleged anonymity of its users, so aggressors tend to think that they are not likely to be identified.

3) It is a very easy thing to do: with a simple "click", with hardly any effort and from anywhere.

An unbalance of power is generated, as the aggressor or aggressors exert their power over their victims with the intention of humiliating them and subduing them. In addition to that, the high availability and easy access to the media used for cyberbullying (social media, blogs, instant messaging…) contribute to its quick dissemination and even lead to loosing control over the images or harmful comments that have been posted.

This kind of situation may seem like a joke to begin with. And usually its potential consequences are not taken into consideration. In many cases, cyberbullying may even end up forcing the victim to attend a different school or to move to a different town. Furthermore, sometimes the aggressor is not identified or his/her identification is difficult, and this may increase the victim's feeling of defencelessness.

In many occasions the aggressors are specifically active in cyberspace, i. e., when they are facing a screen they'll say and do things they would never say or do in a face-to-face situation. Among the media used in cyberbullying, we can highlight sending text messages with threats or false rumours, stealing passwords and identities in order to denigrate the victim, pretending to be the victim and telling others about the victim's personal life or insulting schoolmates, transmitting photographs, publishing information in blogs...

Finally, it is important to highlight that many cyberbullying cases are linked to two additional problems. These two other problems have similar characteristics, as they are also of recent appearance and also have very serious consequences: sexting and grooming.

Sexting refers to a situation where young people send to each other sexually explicit messages or photographs using electronic media. Apart from the inherent risk of this action, a serious problem arises if the person who receives these images uses them to blackmail the other person and asks her/him to do something under the threat of transmitting those images.

On the other hand grooming comprises all the actions a person carries out on a minor with a markedly sexual aim. The aggressor's goal is to obtain images of the child in sexual or pornographic situations and even the possibility of physically and personally contacting the child in order to achieve sexual abuse.

3.1.2 WHAT TO DO?

STUDENTS WHO ATTEND THE SAME SCHOOL:

1. The victim must ask for help and inform an adult s/he trust about the situation (parents, teachers, etc.).

2. We must keep evidence of the facts or the existing electronic evidence:
   - a) Saving snapshots.
   - b) Copying the information on a disk, a pen-drive, etc.
   - c) TTaking pictures of the screen using a camera, making sure the date on which the photograph is taken is registered by the camera.

3. We must contact the web or social media Manager, and we must ask him/her:
   - a) STo save the information to be used to support eventual reports to the polices.
   - b) To cancel published images, comments and/or profiless.
   - c) To implement the internal regulations for these cases (if they exist).

4. We must inform the school's heads, and show them the evidence mentioned above. At the same time, we must ask them to intervene in order to settle the conflict, adopting the relevant educational and/or disciplinary measures that will apply to each case.

   Schools have the duty and obligation of intervening according to article 46 of the Spanish Royal Decree no. 732/1995, on the students' rights and duties and the schools' rules for social harmony, which states that: :

   "*Actions that go against the school's rules for social harmony carried out by the students inside the school or during complementary or extracurricular activities may be corrected. Likewise, students' conduct may also be corrected, even if it takes place out of the school, provided it is motivated or directly related to school life or it affects their schoolmates or other members of the school community*".

5. The school, after verifying the facts, must launch an action plan, implementing the relevant measures in order to tackle the conflict situation: with the victim, the aggressor(s), observers, students' families and teachers.

STUDENTS WHO ATTEND DIFFERENT SCHOOLS:

After being informed of a case of cyberbullying in which one of its students is involved, the school must collect all the information available about the facts and intervene with regards to its students (keeping evidence, contacting the social media or web involved, etc.).

Once the information has been verified, and it has therefore been confirmed that there is cyberbullying, the school's heads must:

1. Convey the information to the other school's heads.

2. Contact the Tutor Police Officers, members of the Local Police Department for Children, who will coordinate the actions carried out by both schools, the minors involved and their families. Furthermore, if considered necessary, the Tutor Officers will inform the Regional Ministry for Social Services and any other relevant public bodies in order to solve the conflict.

3. Depending on the type of case, Tutor Officers may inform the Spanish Agency for the Protection of Personal Data.

4. Finally, depending on how serious the case is, it will be communicated to the State's security forces.

3.1.3 HOW TO PREVENT IT?

Of course, new technologies are not a problem per se, and they have also become so important for teenagers that they are not willing to give them up. They consider ICTs essential and their use is perfectly well integrated into their everyday life. It is necessary, nevertheless, to prevent risk situations, and two powerful tools are available for that purpose: information and education. If teenagers get to know the risks and potential consequences of a bad use of ICTs, and if they know how to react and who they can ask for help if they have a problem, surfing the Internet will be for most of them as satisfactory as any other healthy activity.

Although there are specific guidelines and pieces of advice for a correct use of ICTs – which you will find below –, parents, teachers, educators and the society as a whole must bear in mind that there are NOT two separate and parallel lives, a real one and a virtual one. Both worlds are totally interrelated, and what happens in one of them has an impact on the other one. In fact, teenagers themselves say that they see no difference between the two. As a consequence, the same recommendations and guidelines we convey to children about their everyday life are completely transposable to the Net: going from simple good manners up to very evident aspects related to having contact with strangers, etc.

PARENTS

1. Learn as much as you can about the Internet: the family must surf together.

2. Discuss with your children what may be done online and what may not be done online.

3. Limit your children's Internet time: this prevents cyber-addictions and promotes face-to-face relationships.

4. Place the computer in a common room of your home.

5. Advise your children to be careful with the pictures they publish: they may stay forever on the Net and they give a lot of information about them.

6. Inform your children that it is important not to believe everything they read in the Internet.

7. Make sure your children ask for your permission before registering in any Website.

8. Learn about what your children like:
- Their activities (where they go, with whom, etc.)
- Ask about who is behind each contact, each mail…

9. Use filters and antivirus.

TEACHERS

1. Communicate the necessary guidelines about a safe and responsible use of the Internet and the social media during your time with your tutor group:
- Training sessions at school about respecting peers
- Highlight that Internet users are not anonymous.

2. Tell your students that you are a responsible grown up, a member of the school, and that they can ask for your help if they have any problems with other students.

3. Keep an eye out for conflict situations that may lead to cyberbullying.

4. Be familiar with the action protocol in case one of your students is cyberbullied, paying special attention not to make the victim stand out with your intervention.

STUDENTS

1. Do not answer to any threatening or offensive messages. If you receive such messages:
- Keep offensive messages as evidence.
- If you know who sent them ask that person to take them back.
- Contact the website manager and report those messages.
- Ask for help: your parents, form tutors or PROTÉGELES' safety centre: contacto@protegeles.com

2. Take into account that Internet users are not anonymous and there is always track of what one does on-line.

3. Do not give personal information to people you do not trust.

4. Do not upload photographs or videos where other people feature without their permission.

5. Do not open e-mails or attached files sent by strangers.

6. Do not arrange blind dates with strangers.

7. Do not forget that insulting, threatening, stealing passwords, pretending to be someone else, etc. may be offenses.

8. Only accept as friends/contacts people you've met face-to-face.

9. Take into account that the information you upload to the Internet may stay there forever, and that it may be seen by anyone.

10. Passwords must be safe, secret and complex.

11. Do not include any personal data in your e-mail address.

12. Before registering in a Website, ask your parents for permission.

13. Use available settings, such as: "privacy", "block", "report"... in order to be protected online.

14. Do not contribute to vulgar chain messages and do not send collective messages showing everybody's e-mail addresses.

15. If you encounter a problem while surfing: it's essential to ask for help as soon as possible so that it can quickly be stopped.

3.1.4 CONSEQUENCES

An inappropriate use of ICTs may have negative consequences and some of them may even be physical, due to the anxiety these situations, such as cyberbullying, produce: headaches or stomach aches, eating or sleeping disorders... There are also social consequences: isolation, difficulties in social interactions...; and also psychological ones: low self-esteem, feeling of defencelessness, problems to concentrate...

yberbullying may have an even greater impact than normal bullying, because several and very diverse circumstances get together:

- The information or images used are disseminated more rapidly through ICTs
- Dissemination is simpler and free of charge, so it reaches a greater number of people.
- The victim doesn't feel safe anywhere, because unlike bullying, which takes place in a specific place like the school, cyberbullying reaches even the victim's bedroom. A computer, a mobile phone, a tablet or even a games console connected to the Internet may constantly reproduce the harassment situation.
- Frequently other people, who often do not even know the victim, also participate. These people see that someone is been attacked or made fun of and they join in, add their own comments and end up contributing to the harassment

We must take into account that when teenagers are suffering from such a situation through ICTs it is difficult for them to tell about it because:

1. They are afraid of reprisals.
2. They may have been threatened.
3. They are alone and do not trust anyone.
4. They may feel guilty.
5.
6.
7. They do not want their parents to worry.

Just like in common school bullying, teenagers that suffer from cyberbullying may have specific behaviours at school that will offer a hint about what is happening to them. For example, as we mentioned before, they may suffer headaches or stomach aches that make them miss some classes or not participate in class as usual; during the breaks they may be isolated or stay in class instead of going out to the schoolyard, and they will be alone most of the time; their academic performance worsens, as well as their concentration; they may suffer from sudden mood swings and be, in general, sad and apathetic...

Isolation is nurtured by what we call the "code of silence". Very frequently, those schoolmates who are aware of what the victims are going through do not do or say anything. The act that way because they tend to think that it has nothing to do with them, or they become allies with the aggressor as a way of protection, a way of avoiding becoming victims themselves. The spectators' role is essential, as they have the power of intervening and asking an adult for help in order to try and put an end to the situation.

3.2 PRIVACY

Privacy can be defined as the area of an individual's personal life s/he has the right to protect from all sorts of intrusions.

When talking about privacy we must also refer to the Right to a Private Life and to the Protection of Personal Data.

In our days, privacy must be specially protected due to the constant progress and repercussion of new technologies.

3.2.1 RIGHTS AND DUTIES.

The right to personal and family privacy, to honour and one's own image is inherent to every person, it is an inalienable right and it specifies the value of human dignity in a social and democratic rule of law.

The right to a private life is well regulated in different kinds of legislations, both at the international level and at the national one, and in all cases it is considered to be a fundamental right of human beings:

EUROPEAN LEGISLATION::

The Universal Declaration of Human Rights (art. 12) and the International Covenant on Civil and Political Rights (art. 17), adopted by the General Assembly of the United Nations, state that: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everybody has the right to the protection of the law against such interference or attacks.."

LEGISLACIÓN EUROPEA:

The European Directive 95/46 EC of the European Parliament and the Council of the 24th of October on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
Spanish National Legislation:
Art. 18 of the "Spanish Constitution of 1978" establishes the following:

> *"1. The right to honour, to personal and family privacy and to one's own image is guaranteed. 2. The home is inviolable. No entry or search may be carried out without the permission of the head of the household or a court order, except in the case of flagrant offense. 3. The secret of communications is guaranteed, specially in the case of postcards, telegraphs and telephone communications, except if there is a court order. 4. The law will limit the use of IT in order to guarantee the citizens' honour and personal and family privacy and the full exercise of their rights."*

Just like other fundamental rights, the right to privacy becomes a duty with regards to other people. As a consequence, just as we MAY require our privacy to be respected, we MUST respect other people's right to privacy. This premise is transposable to new technologies: users must respect other users' privacy.

It is important to pay special attention to the following issues:

- Publishing our own private information. Depending on the type of information that we provide or post, we may be exposing ourselves to different kinds of risks or dangers (cyberbullying, grooming, etc.)
- Publishing personal information about other people (including tagged images or pictures) without their consent.

3.2.2 DATA PROTECTION: WHICH DATA SHOULD I PROTECT?

In the Law on Data Protection personal data are defined, without limitation, as any kind of numerical, alphabetic, photographic or acoustic information about an identified or identifiable individual and which may be collected, registered, processed or transmitted.

Therefore, our personal data define our right to privacy and, as a consequence, are part of our private life. No one may obtain our personal data if we do not provide them of our own will. Depending on the amount and kind of personal data we provide, we will be exposing our private life and privacy to a greater or lesser extent.

Nowadays, privacy reaches a special and different dimension, as a consequence of the massive use of new technologies, the Internet and, more precisely, social media. These networks have become important sources of information about all their members and users. This is why we insist on being careful when making our personal data public.

In Spain, the minimum age for users of social media has been set at 14 years, taking as a basis the Civil Code and the Law on Data Protection, which confer youngsters older than 14 years of age the right to give their personal data without their parents' permission. The problem is that in practice, there are many children under 14 registering or accessing several social media illegally: they just enter a false date of birth. Unfortunately, there are currently no efficient and objective systems to control the real age of users. The control mechanisms currently used are the following:

1. Other users who report under age users.
2. The social media themselves track profiles.
3. Parental control.

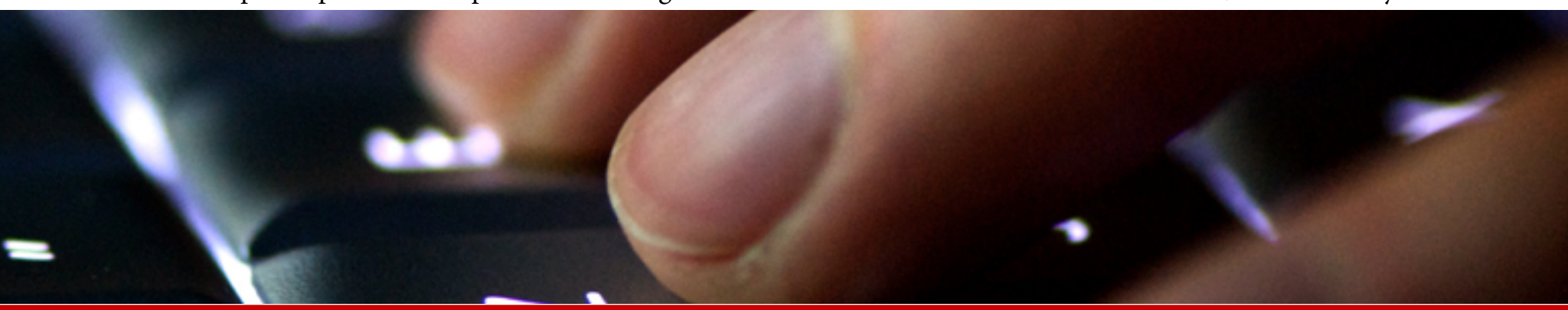
On the other hand, with regards to data protection, users of social media services must bear in mind that they may incur in the following risks:

WHEN REGISTERING:

- We are asked to provide excessive personal data.
- We give our consent and accept that the manager may use our data.
- We often do not restrict the visibility of our data. Private profiles.

WHILE ONLINE:

- We do not control the information and images we post.
- When we publish images (pictures and videos) anyone can copy them, manipulate them and distribute them.
- Images can provide a lot of information that may put the teenagers at risk, as well as their acquaintances and relatives:
- The location of the teenagers may be known.
- Published information may stay online forever.
- In public profiles or in profiles where a great number of friends or users have been added, it is necessary



WHEN UNREGISTERING:

- Eliminating a profile is not the same thing as deactivating it.
- The social media manager keeps the data.

PROTOCOLO ACTUACIÓN EN CASOS DE VULNERACIÓN DEL DERECHO A LA INTIMIDAD:

1. Action protocol in cases when the right to privacy is breached:
   - Printing snapshots.
   - Copying the information on a disk, a pen-drive, etc.
   - Taking pictures of the screen using a camera, making sure the date on which the photograph is taken will be registered by the camera.
2. We must contact the web or social media Manager, and we must ask him/her to cancel personal data, comments and/or texts and to save the information so that it can be used to support potential reports to the police.

3. We must contact search engines that may have indexed the contents asking for those contents to be blocked or taken away.

4. We must report the case to the Spanish Agency for Data Protection.

5. We must start civil and/or criminal proceedings.

3.2.3 OFFENSES.

In many cases the infringement of somebody's right to privacy may be an offense. We will now describe some of the most frequent offenses::

Discovery and disclosure of secrets: The situation where someone, in order to discover o infringe somebody else's privacy, without his/her content, takes hold of their e-mail or of any other documents or personal effects, or intercepts their communications or uses technical devices for hearing, transmitting, registering or playing sound, image or any other communication signal.

Insults: Actions or expressions which harm somebody else's dignity, discrediting his/her reputation or making an attempt against his/her esteem. For example: Disseminating private images or videos, insulting, disseminating photomontages, etc.

Falsifying a private document: Subscribing somebody else (the victim) to a mailing passing to be that person; sending a huge number of subscription mails using that person's identity.

Fraud: People who, for profit, use sufficient deception as to deceive their victim, leading the victim to do something that will be harmful to himself/herself or to others. For example: Manipulating data or software in order to obtain an illicit gain.

4. UNIDADES DIDÁCTICAS

Each of the following teaching units is composed of a series of activities designed to be carried out during teaching hours. These activities last about 45 or 50 minutes. Obviously, before actually starting these activities we recommend the teacher to spend a few minutes promoting an atmosphere that will encourage learning. In some teaching units several activities are proposed, trying to cover most of the unit's contents and offering an opportunity to adapt to the specific needs of each group, thanks to the different options available. These activities can therefore be carried out independently one from the other.

GENERAL GOALS

CYBERBULLYING

- Getting to know and learning to identify the phenomenon of cyberbullying.
- Giving guidelines for action in such a situation.
- Providing tools to prevent cyberbullying.
- Highlighting the importance of teaching how to approach this phenomenon and of the teacher's role.

PRIVACY IN THE INTERNET

- Getting to know the basic safety rules in the Net.
- Informing about teenagers' rights and duties.
- Conveying the importance of protecting personal information.
- Warning about the offenses that are committed through the Internet.

TEACHING UNIT 1

BASIC SAFETY ELEMENTS

ACTIVITY: PASSWORD BRAINSTORMING

OBJECTIVES

1. Emphasising the importance of creating safe, secret and complex passwords as one of the main Internet safety rules.

2. Giving advice on how to create adequate and safe passwords/nicknames/e-mail addresses.

3. Reflecting on the consequences of including personal data in passwords, nicknames and e-mail addresses.

CONTENTS

1. The importance of having safe passwords as a way of protecting privacy.

2. How to create safe, secret and complex passwords.

3. The risks implied in using personal data in the Net.

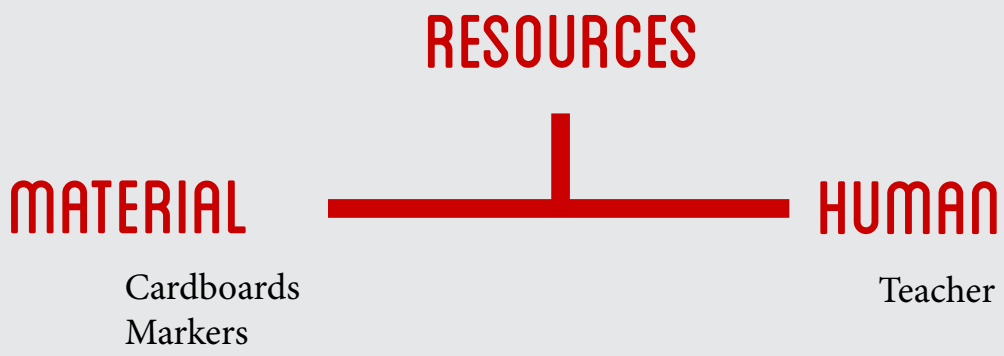
The teacher starts the activity explaining that it is very important to use safe passwords (see bellow "Additional information for the teacher"). The teacher may use a comparison and explain that a password is like the key to a home, and that it can be used to close the door tightly and prevent people you don't want to see from coming in.

The students will be asked to form groups, of a maximum of 5. The teacher then explains the students that one of their schoolmates is going to create an e–mail account for the first time. What advice would you give him/her for his/her password to be safe?

Each group must write the examples they can think of on a cardboard. A spokesperson per group will explain

their pieces of advice to rest of the students.

With everybody's ideas a list will be drafted including the best pieces of advice, which are the ones they must also take into account for their own passwords.



ADDITIONAL INFORMATION FOR THE TEACHER

In many occasions, when we think about the safety of our personal data, we forget the very important role passwords, nicknames and e-mail addresses play. This is why it is key to remember the following guidelines:

For passwords:

- They must be secret, complex and safe.
- You must never share your passwords, except with your parents.
- For a password to be safe and complex it must include numbers, letters (capital letters and lower-case) and signs. An idea to create a good password would be to use the acronym obtained from a phrase from a book or a song you like. Ex.: "And They Lived Happily Ever After" Atlhea7_
- Never use as a password data that other people may know about you: your telephone number, your National Identity Card number, your date of birth, the name of your dog/pet…
- Nicknames and e-mail addresses:
- Should not include any personal information that can be used to identify you.
- Ex.: carolina14@hotmail.com. Just by having a look at this e-mail address we immediately know we're dealing with a girl called Carolina and that she probably is 14 years old.
- We recommend you to have two e-mail accounts: you should use one of them only with family and friends and the other one for subscriptions, like to download videogames.
- It is important to keep your contacts private, and not to send e-mails that show other addresses. If you wish to send an e-mail to several people, use the option "blind carbon copy" (BCC, or CCO in Spanish acronyms).

TEACHING UNIT 2

BASIC SAFETY ELEMENTS

ACTIVITY: WHY DID THE PURCHASE COME OUT SO BADLY?

TIME: 45-50 MINUTES | AGE 10-13 YEARS

OBJECTIVES

1. Warning about the existence of Websites you cannot trust.
2. Getting to know how to distinguish between safe sites and non safe sites. Reflecting on the consequences of providing personal data when you register in a Website or in the Internet in general.
3. Giving guidelines that should be taken into account before subscribing to any Internet service.
4. Characteristics of safe Websites.
5. The risks implied in using personal data in the Net.
6. Basic concepts about the safety of personal data.

DEVELOPMENT

This activity will be carried out using a short story where a child is swindled (see bellow "Additional information for the teacher"). Afterwards, in groups, the students must answer questions about the text, and the teacher will finish the session with a discussion and the moral of the story.

Marcos has received in his e-mail address an e-mail and he is very happy when he reads the subject of the e-mail: "REBATES IN YOUR FAVOURITE GAMES!!". Marcos quickly accepts it and opens the e-mail, clicks on the link included in the e-mail and a Website immediately opens: it seems to be the Website he visits with his father to buy his games. Excited and eager to get the huge discount he is being offered, he decides not to wait for his father to do the purchase. In order to buy the game, he is asked to give a mobile phone number and so he does, without realising that he is in fact subscribing to a service with a charge. From that moment on, he will receive text messages with the latest news about games and he will be charged for that in the telephone bill.

As it was an electronic download, Marcos is surprised not to have received the game, although he has indeed received a huge number of messages advertising games. After a few days, his father receives the telephone bill and is very surprised to see the high sum that is due.

QUESTIONS FOR THE DISCUSSION:

- Why did Marcos' father receive such a high bill if they have not called much and they have not sent text messages? What is going on?
- What would you have done in Marcos' place?
- How can we prevent this kind of situations?
- Think about a positive version of this story.

ADDITIONAL INFORMATION FOR THE TEACHER

What is phishing? Phishing is an electronic scam where a user obtains, in a fraudulent manner, another user's confidential information (credit card number, e-mail account password, mobile phone number, etc.).

- The first rule to bear in mind is: never open e-mails from strangers.
- Never provide personal data in Webpages that are not trustworthy.
- Never subscribe to any Website without your parents' permission.
- Websites that are considered to be safe are the ones that show a lock and/or https in the address bar (the "s" in https indicates it is a safe page).

TEACHING UNIT 3

WEB PAGES

ACTIVITY: DONT BELIEVE EVERYTHING YOU READ!

TIME: 45-50 MINUTES | AGE 11-12 YEARS

OBJECTIVES

1. Generating in teenagers a critical view of the information circulating in the Internet.

2. Working on issues related to copyright.

CONTENTS

1. • The importance of comparing several sources of information.

2. • Copyright.

DEVELOPMENT

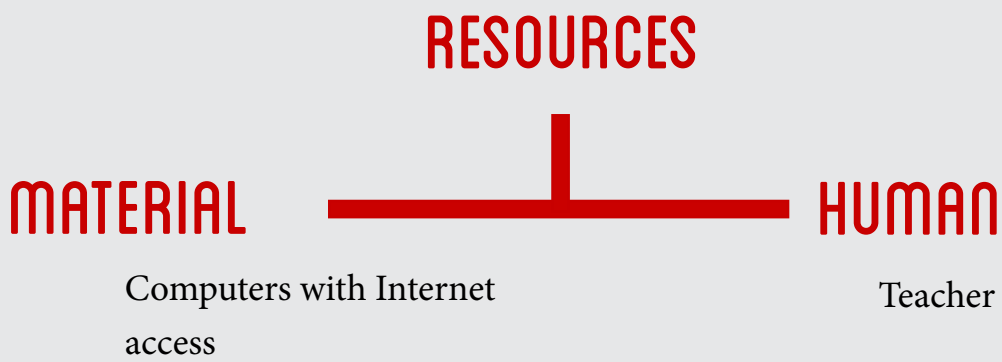
The teacher chooses a simple topic (For example: “Why do seasons change?”) so that the students, in groups and searching in the Internet, prepare a project on that topic.

They are informed that the goal of this activity is to provide the most truthful and corroborated information possible.

Once the projects have been completed, the groups compare differences and similarities in their projects and they analyse where those differences or similarities come from.

The teacher must highlight the importance of:

- Not trusting the first information you find in your search results.
- Not believing everything that is published in the Internet, as not everything is true.
- Using websites of official institutions, like ministries, official professional associations…
- Specifying the sources (copyright).


RESOURCES
MATERIAL
HUMAN
Computers with Internet access
Teacher

TEACHING UNIT 4

CIBERBULLYING

ACTIVITY: ITS NOT KIDS STUFF.

TIME: 45-50 MINUTES | AGE 10-13 YEARS

OBJECTIVES

1. Informing the students about the phenomenon of cyberbullying and its consequences.
2. Giving guidelines for action in this situation.
3. Waking and promoting the empathic capacity of the students so that they can put themselves in the place of those who are causing or suffering from cyberbullying.
4. Promoting mutual help.

CONTENTS

1. Definition and characteristics of cyberbullying.
2. Psychological and legal consequences.
3. Guidelines for action so that students can react in a cyberbullying situation.

DEVELOPMENT

VIDEO PROJECTION

http://beta16.contrapositive.net/resources/cyberbullying/films/es/lfit-film.aspx

QUESTIONS FOR THE DISCUSSION:

To start the discussion:

Do you agree that this situation is a case of cyberbullying? Why?

Who intervenes? Who are the main persons involved in a situation of cyberbullying?

Questions about the development of the conflict:
When and how does the problem start?
What forms of abuse are used? Can you think of any other form of abuse that could be used in cyberbullying?
Let's see what each of the figures said or did in relation to what happened:

Leader aggressor. When she was asked why she behaved like that she excused herself saying it was just a joke, that everybody laughed and that it's not such a big deal! What do you think about her?

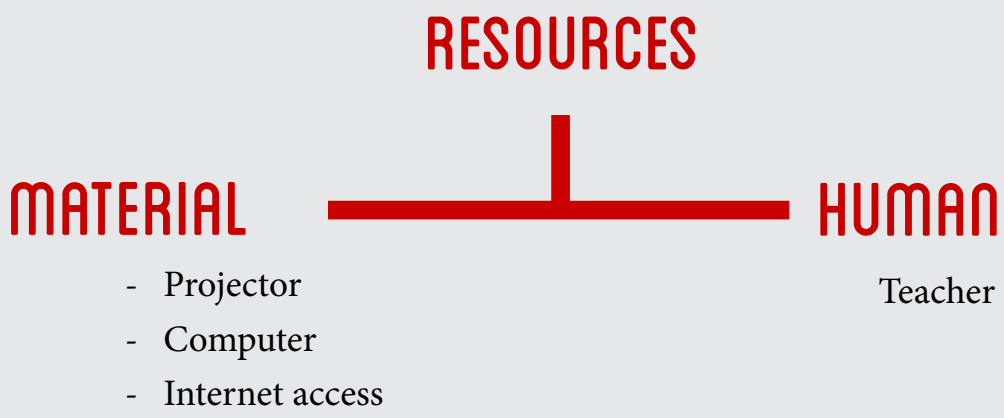
Observers. When observers are asked about their behaviour, they excused themselves saying that everybody laughed at Joe, although one of them said that he realised Joe was having a hard time and stopped laughing at him… Do you think he could have done something else? If a schoolmate is going through the same kind of situation as Joe, is it enough not to laugh at him when others do so to feel that you are not contributing to his situation?

Teacher. The teacher said that she noted that Joe had changed and seemed sad and stressed, but, when she asked him directly Joe said nothing was wrong with him. Could the teacher do something to help him if no one told her what was going on?

Mother. The mother went to the school and talked to the Headmistress. Did she do the right thing?

Victim (Joe). Do you think Joe did the right thing deleting/hiding the messages?

Questions about the outcome of the conflict:
What would you do if you were the victim? And if you were an observer?
Why doesn't the victim ask for help?



TEACHING UNIT 5

CIBERBULLYING Y REDES SOCIALES

ACTIVITY: CARMENS STORY

TIME: 45-50 MINUTES | AGE 10-13 YEARS

OBJECTIVES

1. Informing the students about the phenomenon of cyberbullying and its consequences.
2. Giving guidelines for action in this situation: asking for help.
3. Waking and promoting the empathic capacity of the students so that they can put themselves in the place of those who are causing or suffering from cyberbullying.
4. Promoting mutual help.

CONTENTS

1. What is cyberbullying?
2. Difference between “telling on somebody” and “asking for help for somebody”.
3. The importance of breaking the “Code of silence”.

DEVELOPMENT

This activity may be carried out in several ways, either in groups, who will give their responses to the issues presented by the teacher, or individually, so each student fills in a sheet previously distributed by the teacher.

You need to access the videos available on the educational platform. Phase I videos will be shown and the students (in groups or individually) must choose one of the options given as possible responses. Afterwards the conclusions of each of the options will be analysed.

Then the teacher does the same thing with Phase II videos.

FASE I:

Some of Carmen's schoolmates have created a profile in Facebook, impersonating Carmen's identity, a girl in class who doesn't have many friends and on whom they pick a lot. Using this false profile, they have insulted other schoolmates, who believe it is Carmen who has done so, so they are pretty upset with her. When Carmen goes to school the following day, on top of the usual scorn she gets extra threats and insults.

Possible responses to the situation:

- 1. Carmen should try to clarify the situation and if she doesn't succeed she has no other choice but to put up with the insults until they forget about it all.
- 2. She should tell her form tutor so that he intervenes, because the situation is out of control now that the problem has reached the Internet.
- 3. She can ask a schoolmate with whom she gets on well for help.

Conclusions of each of the responses (video):

- 1. You must never let other people abuse of you. If you can not solve the problem on your own, you must always ask a schoolmate or an adult you trust for help.
- 2. Asking a teacher for help is always a good option.
- 3. When we have problems with our schoolmates, it is very important to count on somebody's help, because that way you will not feel alone and, furthermore, you will get support to solve the problem.

FASE II:

Carmen tried to clarify the situation with her schoolmates, but it was no good. She decided not to say anything to her teachers or to her parents, because she thought things would calm down with time. Three weeks have gone by, but far from improving, her schoolmates go on picking on her. Carmen feels worse and worse and doesn't want to say anything because she's afraid of being called a squealer. If you were Carmen's schoolmate, what would you do?

ALTERNATIVE RESPONSES:

1. I wouldn't say anything because if I did it would be me who would be called a squealer.
2. I would try to talk to Carmen to support her, and we would go together to tell a teacher about the situation.
3. I would try to talk to our other schoolmates so that they know that Carmen is having a hard time.

CONCLUSIONS OF EACH OF THE RESPONSES (VIDEO):

1. Reporting this kind of situations does not imply being a squealer, it means you are asking for help. It is an unfair situation; Carmen is alone facing a big group of schoolmates and it is difficult for her to settle the situation on her own.

2. It will do a lot of good to Carmen if you go and talk to her, as she will feel she has some support. Furthermore, if you encourage her and you both go together and ask a teacher for help, you will be behaving as a good schoolmate.

3. Trying to talk to the rest of the schoolmates may be a good option, but if they do not stop harassing her it would be better to talk to a teacher.

TEACHING UNIT 6

SOCIAL MEDIA

ACTIVITY: ELISAS STORY

TIME: 45-50 MINUTES | AGE 10-13 YEARS

OBJECTIVES

- Talking about the positive aspects of sharing information through the Internet.
- Raising awareness about the risks different kinds of information may imply when transmitted.
- Warning and teaching about privacy levels and the clauses users accept when creating profiles in social media.

CONTENTS

- Risks and benefits of using social media.
- Privacy in user profiles.
- Friends vs. acquaintances.
- Controlling information and images.

DEVELOPMENT

This activity may be carried out in several ways, either in groups, who will give their responses to the issues presented by the teacher, or individually, so each student fills in a sheet previously distributed by the teacher.

You need to access the videos available on the educational platform. Phase I videos will be shown and the students (in groups or individually) must choose one of the options given as possible responses. Afterwards the conclusions of each of the options will be analysed.

Then the teacher does the same thing with Phase II videos.

PHASE I:

Elisa wants to make new friends because she lives in a small village where there are not many people her age. She thinks social media offer her a perfect opportunity to do so. That's why she has decided to have a Facebook profile and make it public, as she thinks that way she will have more opportunities to meet people. This will also allow her to chat with her favourite cousin who lives in France. She now has over 400 friends in Facebook, as she accepts most people sending a request to her. She says she has met many interesting people, from many different places, and that she's really looking forward to going back home, going online and telling them about her day. Some of them live not far away from her village, and she's therefore thinking about meeting them personally and having a closer friendship.

ALTERNATIVE RESPONSES:

1. I think it is a great way of meeting people and, if she doesn't have any friends, out of all the people she has accepted, some may become good friends.

2. I do not think it is a good idea to tell people she doesn't know where she lives and what she does. Only the closest people should know about that.

3. Creating her Facebook profile has helped her be closer with her cousin, so I think it was a good idea to do so.

CONCLUSION OF EACH OF THE ALTERNATIVES (VIDEO):

1. Social media help being in contact with people, but as we do not see them face to face, we cannot be sure if they really are who they say they are.

2. It is important to be careful with the personal information we provide through the Internet, as we do not know who may access it and what they may do with it.

3. Social media are a good way of keeping contact with people we know and who are faraway, but we must learn the difference between a friend and an acquaintance, as we may not trust them all in the same way.

PHASE II:

A month has gone by and Elisa has gone on meeting more people in Facebook and adding new contacts. A group has organized several meetings she has attended and they get on really well. But she has started having problems with one of the guys in the group, because he sends many messages to her every day. She asked him to stop doing so. The guy got upset and, as he knows where she lives, because she had told him on Facebook and because she has uploaded pictures of her house, the boy has gone to her village and has even painted on

her house's front wall insulting and threatening her. Elisa doesn't really know what to do. What do you think she should do?

ALTERNATIVE RESPONSES:

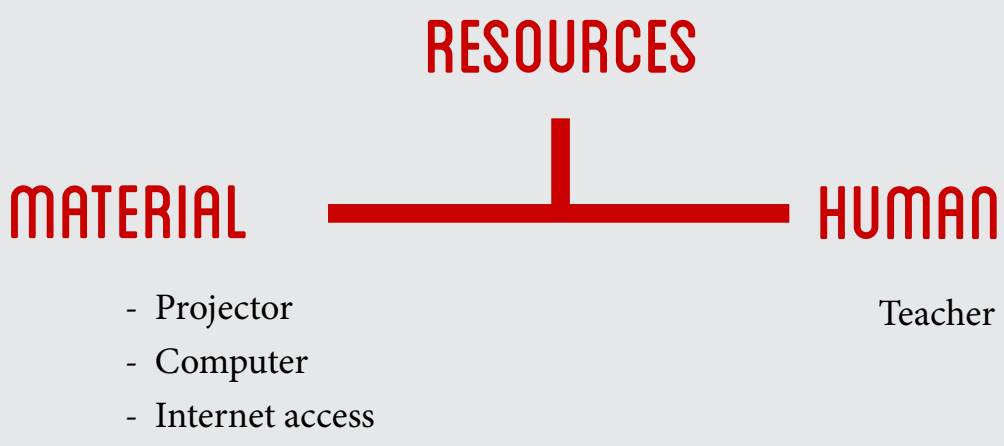
1. Elisa should tell her parents or an adult she trusts (for example, a teacher), so that they can help her find a solution to the situation.
2. Perhaps Elisa should block this boy or report on him in the social network, so that he will not be able to send any more messages to her. That way she can avoid having any more problems.
3. The most adequate thing to do would be meeting him alone to try and talk about the situation and settle it down.

CONCLUSIONS OF EACH ALTERNATIVE RESPONSE (VIDEO):

1. Even if she's afraid of doing so or feels ashamed, it is a good idea to tell her parents or an adult she can trust. Although some adults may not know much about the Internet, they have a lot more experience in solving problems and know who they should talk to and what to do to settle things down.
2. It is fine to block him or report on him in the social network, but he already knows where she lives and problems may therefore continue. That is why she should tell an adult she can trust to help her find a solution. It would also be a good idea not to keep her profile public in Facebook, but allowing only friends to access it in order to avoid this kind of risk situations.
3. As she is already having problems with this boy, meeting him alone would be a high risk situation, as she doesn't know how he may react. If she considers talking with him would be an option, she should only go if accompanied by someone she can trust, and if possible, an adult.

As a conclusion, the teacher may ask the following questions and then finish off with the basic safety guidelines for social media.

1. ¿Which is the safest privacy level? Why? / What does it mean to have a "public profile"?
2. What kind of pictures do you upload to your profile? / Would you put that picture on the notice board at school? Do you think you could loose control over that picture, even if it is protected against downloading?
3. What is the risk of personally meeting people you have contacted through the Internet?



TEACHING UNIT 7

COMPUTER AND MOBILE PHONE

ACTIVITY: DO I KNOW EVERYTHING ABOUT MY MOBILE PHONE?

TIME: 45-50 MINUTES | AGE 11-12 YEARS

OBJECTIVES

- Raising the students' awareness about the need of using this tool in a responsible way.
- Informing about the legal issues a bad use of this tool may lead to.

CONTENTS

- How to use mobile technologies correctly (camera, Internet access, social media…)

VIDEO PROJECTION:

May I take a picture with my mobile phone of whomever I want and without permission?
http://www.youtube.com/watch?v=ylh1zzeICDM
Brief discussion about the content of the video.

Questionaire:

1. May I take a picture with my mobile phone of whomever I want and without permission?.

    a) YES, as long as I know them.
    b) NO, I must always ask for permission

2. May I post in the Internet the pictures I took of my friends using my mobile phone?

    a) NO, maybe some of them do not want their image to be uploaded to the Internet.
    b) YES, if they let me take a picture, I can do whatever I want with it.

3. Is it safe to have pictures stored in my mobile phone?
    a) YES, only I have access to my mobile phone.

b) It depends on the type of photograph.
c) It is not totally safe because if I loose it or it is stolen anyone would have access to that information. It is also dangerous if I connect it to public Wi-Fi networks.

4. If you receive an MMS (video) depicting a practical joke on a schoolmate, what do you do??

a) I send it to my other schoolmates because it's really funny.
b) I delete it immediately.
c) I tell my teacher/parents so that they can help him/her.

5. When you change your mobile phone (device) for a new one you must remember to:

d) Take the memory card out.
e) Delete the information stored in the telephone and to take the memory card out.
f) Delete the information stored in the telephone and to take the memory card out.

6. If you receive a message from a contact that you do not know telling you to download a file…

a) you open it to see what it is.
c) you do not open it, as you are not sure it is safe to do so.

Without collecting the questionnaires, you discuss with the class the correct answers, so that each student may reflect about the options s/he chose. The teacher will tell the students which are the correct answers and why.

RESOURCES

MATERIAL

- Questionnaire
- Pens

HUMAN

- Teacher

TEACHING UNIT 8

GROOMING

ACTIVITY: WHO IS WHO?

TIME: 45-50 MINUTES | AGE 10-13 YEARS

OBJECTIVES

1. Informing about the potential risks implied in talking to strangers through the Internet.
2. Preventing potential sexual harassment situations.
3. Getting to know the resources available to face this kind of situations.

CONTENTS

1. How grooming takes place: prevention and identification.
2. What to do when facing this kind of situations.
3. Resources and places to go for help.

DEVELOPMENT

One of the students will be invited to cooperate in this activity as a volunteer. The volunteer will be taken out of the classroom and the teacher will explain the instructions to him: he must pass for somebody else. In order to be able to do so, he will be given a photograph of an adult man and he is not allowed to show it to the rest of the class. He will have to answer to the questions asked by his schoolmates, who will try to discover who he is. He must lie about the character's identity so that they do not discover he is in fact an adult. Likewise he will ask questions to them and get them to give him personal information. The teacher will offer the volunteer the following questions for him to use:

- How old are you?
- What school do you go to?
- Do you practise sports? Are you in a federation? Where do you usually practise sports? Etc.
- Do you live close to your school? Do you walk to school?
- Do you have a profile in a social network? I'll tell you my username, will you tell me yours?

Once the volunteer has understood his role, the teacher brings him back to the classroom to start the activity.

While the students answer the volunteer's questions, the teacher will take note of all the personal information they give him.

After all questions have been asked, the teacher will show the students the picture of the volunteer's character. They will realise that the volunteer has lied to them and they have answered to his personal questions with the truth and trusting him. A discussion will start about how to prevent and identify this kind of people in the Internet, focusing on the fact that if something like this happens to them or if they have doubts about somebody, they must tell their parents about it.

The conclusions must lead to understanding that:

1. In the Internet not everybody is who they say they are.
2. Receiving somebody's picture by mail or seeing somebody's image with a Webcam does not mean that those images truly correspond to that person.

RESOURCES

MATERIAL

- A picture of an adult

HUMAN

- Teacher

TEACHING UNIT 9

GROOMING

ACTIVITY:LAURAS STORY

TIME: 45-50 MINUTES | AGE 10-13 YEARS

OBJECTIVES

1. Informing about the potential risks implied in talking to strangers in the Internet.
2. Preventing potential sexual harassment situations.
3. Getting to know the resources available to face this kind of situations.

CONTENTS

1. How grooming takes place: prevention and identification.
2. What to do when facing this kind of situations.
3. Resources and places to go for help.

DEVELOPMENT

This activity may be carried out in several ways, either in groups, who will give their responses to the issues presented by the teacher, or individually, so each student fills in a sheet previously distributed by the teacher.

You need to access the videos available on the educational platform. Phase I videos will be shown and the students (in groups or individually) must choose one of the options given as possible responses. Afterwards the conclusions of each of the options will be analysed.

Then the teacher does the same thing with Phase II videos.

Para llevarla a cabo hay que acceder a los vídeos de la plataforma educativa. Se visualizarán los vídeos de la Fase I y los alumnos (por grupos o individualmente) deberán elegir una de las alternativas de respuesta y se analizarán las conclusiones de cada una de ellas.

Posteriormente se hace lo mismo con la Fase II.

PHASE I:

My friend Laura says she has met a boy in the Internet. She is quite shy and finds it difficult to make friends, but says that in the Internet she feels freer to say what she feels and that is the reason why she likes talking to this boy. Laura doesn't have too many friends and she is becoming more and more excited about talking to this boy. As they haven't met in person yet, the boy has sent his picture to her and he has asked her to do the same thing. My friend doesn't know what to do.

ALTERNATIVE RESPONSES:

1. Laura may send pictures to him because she has already been taking to him for quite some time, and on top of that they fancy each other. Exchanging photographs is the normal thing to do; that way they will know what they look like, as somebody's appearance says a lot about the person.
2. I don't think it is a good idea to send any photographs. You do not really know who he is or what he intends to do with them.
3. She can send to him pictures of a friend of hers, who she considers very beautiful, so that he will still fancy her, and she can tell him the truth later.

CONCLUSIONS OF EACH ALTERNATIVE RESPONSE (VIDEO):

1. It is true that photographs give a lot of information about people and that is precisely the reason why you must be careful when choosing the photographs you are about to send.

2. It is possible to meet interesting people in the Internet, but you must bear in mind that not everybody is who they pretend to be, and that's why it is important to be cautious. You must be aware of the fact that it is easy to deceive others by sending somebody else's pictures and therefore you should not trust everybody.

3. Sending a photograph pretending to be the person on the pictures is an offense, and in addition to that you may put that person at risk.

PHASE II:

My friend Laura keeps in contact with the boy she met in the Internet. She trusted him because they talked a lot and they told each other everything about their lives. So she has now decided to meet him in person. At school everybody knows about this and some of Laura's schoolmates are picking on her saying she finally has a boyfriend. Laura doesn't care because she feels she has met someone special who understands her better that their schoolmates do. They are going to meet one of these days after school.
What would you say to Laura?

Alternative responses:

1. Laura can go to that date without any concerns because she has been talking to this boy for quite some time. It's a great opportunity to meet someone she fancies and with whom she gets along pretty well. No doubt that she should go!!

2. She can go to the date but a friend should go with her.

3. I do not think she should go to the date, because she doesn't know who she is going to meet. It could be dangerous.

Conclusions of each alternative response (video):

1. The truth is she has never really seen that boy and she doesn't know who he is. Even if he sent a picture to her, perhaps it wasn't him on the photograph. A "blind date" may be a dangerous situation if Laura is alone. If she wants to go she should ask someone she trusts to accompany her and, if possible, it should be an adult.

2. A way of avoiding problems in a "blind date" is to go accompanied by someone else.

3. Many people use the Internet to deceive other people. They pretend to be somebody else. In this case, instead of being a boy, it could be an adult or a bunch of boys who want to make fun of Laura.

TEACHING UNIT 10

SEXTING-SEXTORTION AND GROOMING

ACTIVITY: : I THOUGHT S/HE FANCIED ME

TIME: 45-50 MINUTES | AGE 11-12 YEARS

OBJECTIVES

1. Explaining what sexting and sextortion are.
2. Getting to know what to do if you become a victim of sextortion.

CONTENTS

1. What sexting and sextortion are.
2. Guidelines on what to do.

DEVELOPMENT

Students are distributed into groups and they receive a copy of the text bellow. Once the story has been read, they must answer the questions included bellow the text.

Afterwards, all the students must participate in a discussion in order to reach common conclusions focusing on the main rules that must be applied to avoid this kind of situations:

STORY NO. 1:

My name is Carmen and I am 13 years old. This year, in class, there was a new boy, very handsome and whom I really fancied. Many of my friends also fancied him, but he was only interested in me. Besides talking a lot in class, when we got home we chatted a lot and sent messages to each other using WhatsApp. In the end we started going out together. One day I thought he would like having a more intimate photograph of me, so I took a picture of myself wearing only my underwear and I sent it to him. He liked it so much that he asked me for more. I sent him some more and even one or two where I was not wearing a bra. After some months going out together I decided to split up and he didn't seem to like that at all. He has threatened me saying he will pass those pictures along if I do not get back together with him. I don't know what to do.

Questions for the discussion:

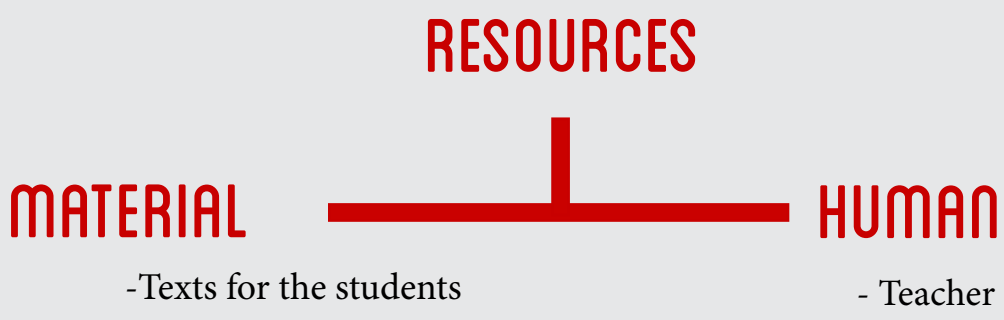
- Do you think she should get back together with him?
- Can Carmen be sure that if she gets back together with him he will not pass her pictures along?
- What do you think Carmen should do?
- Do you think Carmen's problem is due to the fact that she didn't find the right boy she could trust?

STORY NO. 2:

Beatriz (fictitious name), who had just turned 13, found refuge in social media. The situation at home was not very good and economic problems made coexistence quite difficult. She enjoyed meeting new friends, with whom she shared her thoughts, concerns and some laughs. "I spent many hours at the computer, chatting here and there. In one of the chats I found a boy with whom I talked a lot and I ended up giving him my e-mail address. He asked me to send a picture of me, so he could see how I look like and I accepted. He said I was very beautiful and he also sent his photograph to me. We went on chatting for some time and he told me he really fancied me. He asked me to send to him a picture of myself in my bikini and so on, little by little. And one day I found myself sending more compromising photographs to him. Then he asked me to appear on the webcam… And I did so…to start with I was wearing my clothes and then he asked me to undress so he could see me, because he said he really fancied me…The truth is I also fancied him…and that is why, one day, when he asked me to show him my breasts…, I did it without really thinking much about it… Then I said no when he asked for more. He didn't like it when I said no, and that is when he started threatening me. He said he would pass along my photographs and videos all over the Internet, to all my contacts, if I refused to show him my body entirely naked. In the end, I gave in under this blackmailing because I was afraid".

Questions for the discussion:

- When you meet someone in the Internet, do you think there is some way of making sure it is somebody you can trust?
- Is it dangerous to send photographs through a mobile phone or the Internet?
- What other options did Beatriz have when the boy asked her to undress in front of the Webcam?



TEACHING UNIT 11

ORGANIC LAW ON THE PROTECTION OF PERSONAL DATA AND IMAGE RIGHTS.

ACTIVITY: COMPLYING WITH THE LAW

TIME: 45-50 MINUTES | AGE 11-13 YEARS

OBJECTIVES

1. Understanding what personal data are.
2. Getting to know what personal data we should give and to whom.
3. Getting to know what personal data shouldn't be given because doing so would imply a privacy risk.
4. Respecting other people's right to privacy.
5. Conveying the need to be especially careful when processing images.

CONTENTS

1. Rights and duties with regards to privacy.
2. Organic Law on the Protection of Personal Data.
3. Internal regulations of social media.

DEVELOPMENT

Students must understand that, in our quality as citizens, we are entitled to a series of rights which protect us. To start talking about this topic, the teacher may refer to article 18 of the Spanish Constitution and underline the protection of personal data.

What are personal data? List the main data that identify a person and which must therefore be protected.

What do the students understand by the phrase "protection of personal data, image rights, private life and privacy"? This question must be asked to the group as a whole so that each of the students has the opportunity of offering their own ideas, and so that the subject may be discussed in detail under the teacher's guidance.

Afterwards the teacher will present the following case studies for the students to solve. They will be asked to determine whether the following situations violate their right to privacy or somebody else's right to privacy or not.

1. During the registration process, a social network asks me to provide the following data: name and surname, date of birth, city of residency, e-mail address, religious beliefs, information about your health and political ideology.
2. I take a picture of my family during Christmas' dinner.
3. I send an e-mail to all my schoolmates adding their e-mail addresses to the CC field.
4. A friend has posted a photograph of me in his profile, where he has 350 friends.
5. Someone stole my e-mail password and now reads the content of my e-mails.
6. I let a friend of mine read the e-mails a schoolmate sends to me.
7. During the break, a teacher tripped over and fell. I thought it was so funny I filmed it with my mobile phone and uploaded it to YouTube so that my schoolmates can watch it.
8. I receive a photograph of a schoolmate in her underwear through WhatsApp with a message saying "Pass it on" and I send it to other people.
9. I register in a games site and, in order to do so, I am required to provide my name and date of birth.
10. A friend accesses her Tuenti profile from my computer and marks the option "remember my password". As I can enter her profile, I have a look at it everyday.

Solutions:

- It is a violation of privacy.
- It is not a violation of privacy.
- It is a violation of privacy.
- It is a violation of privacy.
- It is a violation of privacy.
- It is not a violation of privacy.
- It is a violation of privacy.
- It is a violation of privacy.
- It is a violation of privacy.
- It is a violation of privacy.

RESOURCES

MATERIAL

- Questionnaire
- Pens

HUMAN

- Teacher

TEACHING UNIT 12

CYBERBULLYING

ACTIVITY: CARLOS STORY

TIME: 45-50 MINUTES | AGE 10-13 YEARS

OBJECTIVES

- Informing the students about the phenomenon of cyberbullying and its consequences.
- Giving guidelines for action in this situation.
- Waking and promoting the empathic capacity of the students so that they can put themselves in the place of those who are causing or suffering from cyberbullying.
- Promoting mutual help.

CONTENTS

- What cyberbullying is: examples of this kind of situations.
- The importance of asking adults for help.

This activity may be carried out in several ways, either in groups, who will give their responses to the issues presented by the teacher, or individually, so each student fills in a sheet previously distributed by the teacher.

You need to access the videos available on the educational platform. Phase I videos will be shown and the students (in groups or individually) must choose one of the options given as possible responses. Afterwards the conclusions of each of the options will be analysed.

Then the teacher does the same thing with Phase II videos.

PHASE I:

Carlos has a Facebook profile where his schoolmates are added. He had a problem with one of them the other day during the break: they insulted each other and the other boy threatened him saying he would make his

life miserable. Carlos didn't pay any attention to that, but the boy has created a Facebook group called "I hate Carlos" and there are more and more people in it.

POSSIBLE RESPONSES TO THE SITUATION:

1. If I were Carlos I would create another group hating that boy, and that way he'll know what it feels like. I would give him a taste of his own medicine.
2. The best thing to do is nothing; just let things calm down. This is just because the quarrel is recent; it will all soon be forgotten.
3. He should tell one of the teachers so he gets punished.

CONCLUSIONS OF EACH OF THE RESPONSES (VIDEO):

1. The other boy may feel bad, but it is very likely that he will get even more upset and that the situation will get worse. And even if it is only a way of reacting to a previous insult, insulting or threatening somebody through social media is an offense.

2. Perhaps Carlos' schoolmate ends up regretting what he has done and after a few days he may eliminate the group, so the problem will stop there. But we must bear in mind that many people may have seen the comments in the group and this may cause Carlos many problems.

3. It is a good idea to ask an adult for help, in this case a teacher, although the purpose of talking to a teacher should not only be punishing the other boy, but mainly helping them find a solution to the conflict.

PHASE II:

Carlos continued having problems with one of his schoolmates. The group called "I hate Carlos" was deleted, but one of these schoolmates got very angry because he was punished and decided to upload a photograph were Carlos didn't look very good and started making humiliating comments.

POSSIBLE RESPONSES TO THE SITUATION:

1. He shouldn't say anything; otherwise the next thing they do to him might be even worse.
2. Carlos should upload a picture of that schoolmate and also make negative comments, so he will learn the tough way.
3. The best thing to do is tell his teacher again, so that the school takes measures and, if necessary, may contact the boy's parents.

CONCLUSIONS OF EACH OF THE RESPONSES (VIDEO):

1. PPerhaps he will stop picking on Carlos, although he will most probably continue doing so. Putting up with teasing never is a good solution.

2. This kind of reactions usually make things worse. Carlos must remember he has the right to defend himself, but not in the same way. The correct thing to do would be asking to be left alone or asking for an adult's help.

3. This is a very adequate way of responding in this sort of situations, as this is not something Carlos can solve on his own. He needs help from adults.

TEACHING UNIT 13

SETTING UP PRIVACY IN SOCIAL MEDIA

ACTIVITY: ONLY FOR MY FRIENDS!

TIME: 45-50 MINUTES | AGE 12-13 YEARS

OBJECTIVES

- Making students aware of the need of protecting their privacy within social media.
- Learning to manage the basic elements of a profile's privacy settings.

CONTENTS

- Negative consequences of not protecting privacy in social media.
- Main privacy settings in a social network's profile.

DEVELOPMENT

Before starting this activity with the students, the teacher will need to create a profile in a social network. It should not be a personal profile and it could be called, for example, Class 6A. It is not necessary to upload any specific content to it. The idea is that, using this profile, the teacher will be able to show to his students the different privacy settings in that specific social network.

While explaining each privacy setting, the teacher must discuss with his students the potential dangers the user may be exposed to if those settings are not selected.

The basic options to be shown by the teacher are the following:

1. Overall privacy of the profile
2. Who may publish in your biography? Who may see what others publish in your biography?
3. Disabling public search (not available in all social media)
4. Blocking people, invitations and events
5. All these options can be found in the section called "Privacy settings"

Overall privacy of the profile

- LThere are three different types of profile's privacy: Public, Friends or Customized.
- The Public option: you should never choose this option, as this implies that anybody may access your personal information.
- The Friends option is one of the most adequate ones, as only your contacts will have access to your personal information.
- The Customized option is the most adequate and safe one, taking into account the fact that in social media the word "friends" also includes acquaintances. So if you customize your profile you will be able to distinguish between your real friends and your acquaintances when granting them access to your personal information.

Who may publish in your biography? Who may see what others publish in your biography?

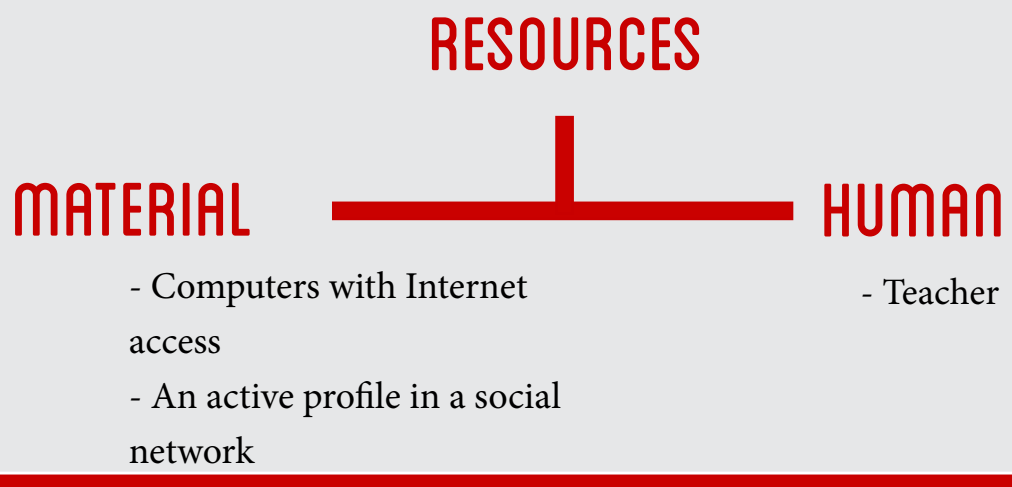
Taking into account that in social media you accept more contacts than what you strictly consider your intimate friends or close friends, this option allows you to control who may publish in your profile.
At the same time, if you allow other people to publish in your profile, you may configure this in a way that will hold the post until you can check it is adequate and approve it.

Disabling public search (not available in all social media)

One of the most common mistakes when protecting our private information is not taking this option into account. Social media users who protect their data using a private profile "only for friends" or even "customized", usually ignore that it is possible to find a preliminary view of their biography and their profile picture in public search engines.
In order to prevent this you must look for an option called Public Search among your "privacy settings" and select "disable public search". This way no-one will access that preliminary view of your biography if they search your name in a search engine.

Blocking people, invitations and events

This may help you prevent a situation where someone you do not want to have among your social network's contacts can contact you sending invitations to you or invitations to participate in events. This is something you can do if you are getting friend requests from strangers or if one of your contacts is bothering you.
You must be careful while managing this option, because even if you block somebody, that person may still contact you if you both participate in common apps, games or groups.



5. RESOURCES

www.protegeles.com
www.internetsinacoso.es
www.acosoescolar.info
www.quenoteladen.es
www.ciberfamilias.com