Content Unit

Parental Control

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: UDIMA
Last processing date: 24.8.2020

Funded by the
Erasmus+ Programme
of the European Union

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

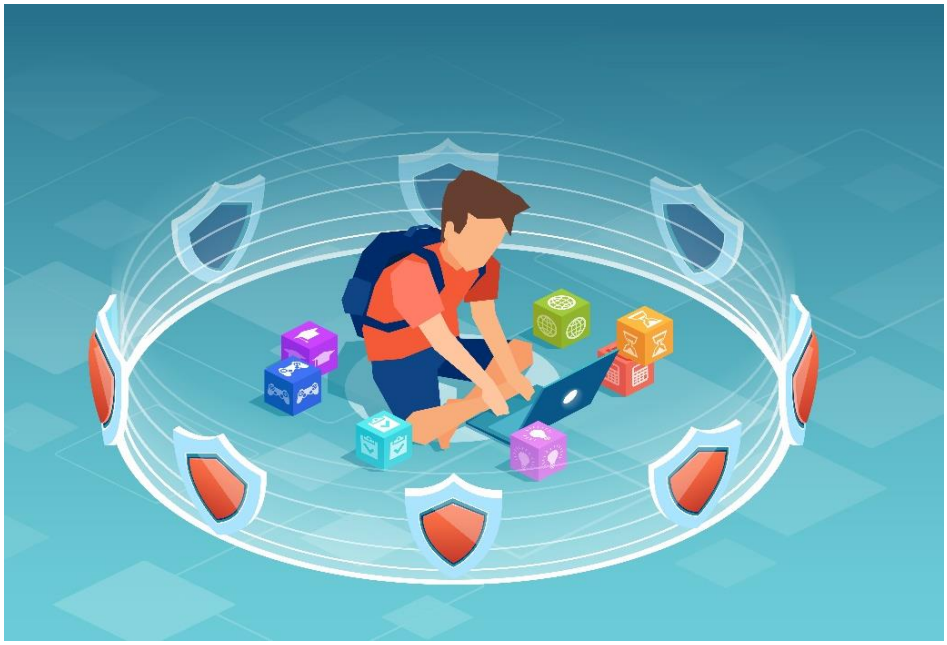
Parental Control

First introduction

Exercising parental control in order to guarantee the safety of the minors in their care has always been one of the functions of parents and guardians. Nowadays this function is expected to be carried out by them and becomes even more important.

They can face numerous dangers such as sexting, grooming, cyberbullying, netholism, and disclosing information. These dangers consist of exposing or being exposed to sexual content, being harassed by an adult, being bullied, becoming addicted to the Internet, or having their data exposed.

All of them can entail negative consequences for the victim regarding their emotional and physical health. Paying attention to these dangers and their first consequences it is possible to establish some tips and detect the problem.



Practical relevance – This is what you will need the knowledge and skills for

After learning this content unit, you will know the importance of parental control to protect children and adolescents from dangerous situations they could get involved while using different technological devices.

Overview of learning objectives and competences

In LO_ParentalControl_01 you will learn which are the principals of parental control and its usefulness.

In LO_ParentalControl_02 you will learn what sexting is about.

In LO_ParentalControl_03 you will learn what grooming is about.

In LO_ParentalControl_04 you will learn what cyberbullying is about.

In LO_ParentalControl_05 you will learn what netholism is about.

In LO_ParentalControl_06 you will learn what disclosing information is about.

Learning objectives	Fine objectives
LO_ParentalControl_01: You know the principals of parental control and its usefulness.	FO_ParentalControl_01_01: You know what technological threats affect minors FO_ParentalControl_01_02: You can give the definition for the term “parental control” FO_ParentalControl_01_03: You can explain what parental control is for. FO_ParentalControl_01_04: You know how technological parental control works.
LO_ParentalControl_02: You know what sexting is about	LO_ParentalControl_02_01: You can give the definition for the term “sexting” LO_ParentalControl_02_02: You know the difference between active and passive sexting. LO_ParentalControl_02_03 You know the risks associated with the practice and dissemination of sexting. LO_ParentalControl_02_03 You can explain three sexting prevention strategies.
LO_ParentalControl_03: You know what grooming is about	LO_ParentalControl_03_01: You can give the definition for the term “grooming”. LO_ParentalControl_03_02: You know the phases and characteristics of grooming. LO_ParentalControl_03_03: You can identify the symptoms of a grooming victim. LO_ParentalControl_03_04: You can explain three grooming prevention strategies.
LO_ParentalControl_04: You know what cyberbullying is about	LO_ParentalControl_04_01: You can give the definition for the term “cyberbullying”. LO_ParentalControl_04_02: You can define the roles involved in cyberbullying and its characteristics. LO_ParentalControl_04_03: You know the consequences of cyberbullying for the stalker and the harassed. LO_ParentalControl_04_04: You can explain three cyberbullying prevention strategies.
LO_ParentalControl_05: You know what netholism is about	LO_ParentalControl_05_01: You can give the definition for the term “netholism”. LO_ParentalControl_05_02: You can identify alarm signals about abusive internet use. LO_ParentalControl_05_04: You know three ways to prevent netholism.
LO_ParentalControl_06: You know what disclosing information is about	LO_ParentalControl_06_01: You can give the definition of disclosing information LO_ParentalControl_06_02: You can identify when children are leaking information

	LO_ParentalControl_06_03: You can explain three ways of preventing the information leakage

1. Build knowledge – What are the principals of parental control and why do we need it?

Nowadays, given the great advance of new technologies, children, adolescents and young people have more and more contact with them. In fact, on numerous occasions, they are responsible for teaching the adults around them to use computers, tablets or mobile phones.
It is not possible to separate minors from these technologies, or at least, it is not easy. The use of the Internet has become something necessary in jobs and even in our everyday. The need to teach them how to use technological devices has become a fact and therefore, the need to integrate them into the education system has also been seen. They are, in fact, a fundamental pillar in their education and very useful when looking for information and performing school tasks. Many centers have already included platforms through which they offer online resources to their students, send them homework and even ask them to deliver their tasks through the platform. At this point in which keeping them away from information technologies is so difficult and even counterproductive, it seems appropriate to consider how to protect them.

There are multiple dangers that can affect children, teenagers and youth on the internet, starting with cyberbullying or sexting that can occur with people who they know and are around them (from their school or their neighborhood for instance), and even continuing with external threats, which are those coming from strangers. Unknown people have the possibility of collecting information about minors and contacting them, not always with the best intentions. In addition, technological tools such as mobile phones, laptops or computers give minors access to a large amount of web content that may be completely inappropriate such as violent content, pornography or radicalism. One of the aspects that concern parents the most and that can bring minors to any of the threats mentioned above are social networks. Social networks allow young people such as minors to access them, and, in addition, young people also enter below the age stipulated for their use, because they can easily lie and mark the desired age without any verification being made.

Before the emergence of new technologies, the whole process of curiosity, experimentation, the establishment of new relationships, etc. through which minors go, happened in front of the eyes of everyone else, it was more visible. This is why exercising parental control was much simpler and there were not so many complications to keep the dangers away. That is also why, today, the definition of parental control acquires new nuances and new media, but it still maintains its essence. Parental control is, therefore, defined as:

Definition
Parental Control …the way in which parents supervise and intervene if necessary, to ensure that the experiences and processes of socialization and personal growth of their children occur adequately and without risks to them.

Risks faced by minors have not changed in essence, but the manner and means through which they may be threatened. New forms of risk lead to new forms and methods of parental control to ensure minors' safety.

Example
For instance, children may suffer bullying in the form of insults, rejection, threats, ridicule or dissemination of hoaxes either face to face or through the Internet, spreading faster and further.

A parental control system is a tool that allows parents to control and / or limit the content to which their children can access the internet from their devices, be they computers, mobiles or tablets. There are many different parental tools and they can be used on the minors' devices to stop some actions, pages or contents or to control them from the same device or even from the adults device.

Example
If parents are concerned about the safety of their children, they should consider what devices the child uses and their age. There are applications and softwares to control Internet use, but not all are available on all devices. The child's age will also guide parents to choose one tool or another, as they can expect different things depending on their needs. For the little ones, it could be a suitable tool on the same device to stop content that is not made for children, while for adolescents, it may be necessary to monitor the time on the same device or what they see from the devices of the parents. Parental control tools are available on every device, but if you wanted something more specific, you could find other tools in online stores or app stores or tools offered by insurance and security companies and Internet providers.

In general, the parental control systems that we have today are used to guarantee minors' safety in the network, thus avoiding possible threats and avoiding bad experiences. More specifically, parental control systems are tools that have been designed to block and filter access to different Internet points and to monitor their use. These tools offer more and more functionalities and can be customized and adapted to the needs of the parents. These functionalities can be divided into the following sections:

- Monitoring: To keep track of online activity. It enables the user to analyze where the child enters, generating warnings if he/she enters non-recommended websites.
- Controlling contact with other people: This functionality allows the user to avoid contact of his/her child with strangers, which according to INCIBE (Instituto Nacional de Ciberseguridad), occurs in 40% of minors.
- Limiting the time of use: It allows you to control both the maximum time that the child has access and the time at which he/she has permission to keep the device powered.

- Controlling access to inappropriate sites: It allows the user to control or block access to websites which contents are sensitive for early ages or that compromise their data.
- Restricting applications: This functionality prevents the use or download of certain applications.
- Avoiding online purchases: It is possible to disable the purchase, whether intentional or not, of applications or other online items.
- Geolocation: It allows to know the exact location of the child.
- Second authentication factor: In addition to the password to unlock the device, a code that is sent to the parents is required to unlock the device. This way, parents are the ones who give access to minors at all times.
- Call blocking.

All these forms of parental control are used to guarantee the safety of minors, protecting them from strangers and inappropriate content or pages. They also help protect children and adolescents from their own or others' improper use of the Internet, whether intentional or not. This protection can be carried out by monitoring children's Internet use or by blocking and controlling different functions.

For the little ones, the parental control tools that are usually chosen are those that limit and prevent access to certain contents that are inappropriate for their age or limit the usage time of the different applications and devices. These tools use different techniques to achieve it. Most of them use lists where those sites that should not be seen (blacklists) are filtered or allow access only to those contents that are in the white lists, lists of suitable contents for the little ones. It is also possible to block access to content with certain keywords (pornography, drugs, shopping, etc.), which can result in blocking suitable pages for minors due to false positives. In addition, this kind of parental control tools also allow you to block access to specific applications, allow their use only without access to the Internet, disable the chat function or control the time and schedule in which they are given access.

On the other hand, and thinking of teenagers, there have also been created parental control tools that allow the use of electronic devices and activity monitoring. It comes to a point where children need to use their devices more freely, while their knowledge of these tools increases, and they are curious to know more and to contact other people. From these parental control tools that allow parents to monitor the activity, it is possible to know the services teenagers access, what they do, the people they contact and where they connect. The last is possible thanks to GPS and location techniques that all mobile devices include.

This parental control can be exercised from different points:
- Router and DNS servers (Domain Name System): The router is the digital access of a house and through it, it is possible to manage the navigation restrictions of all the devices that connect to it. From the router

it is possible to control and filter the contents to which they have access and to which all these connected devices have already accessed, mark time limits regarding the connection and apply filters on the web pages. It can also be filtered by DNS servers.

Analysis
This is a good option to control all devices in the house but it may not be the best option if you wanted to set specific restrictions on each device. Also, it is not possible to control devices when they are not connected to the server.

- The device itself: All the devices we have at home (computers, tablets, mobile phones and even toys) include parental control packages and allow blocking access to content that is not suitable and control online activity.

Analysis
As it is included in the device, we do not need to look for other parental control systems and we avoid paying for this service. In addition, it allows us to apply control on each device individually. However, it is not usually possible to personalize and adapt the service to our needs.

- Software: In addition to computer control programs that protect against various dangers that we can find on the Internet such as viruses and malware, it is also possible to block websites, mark time limits or control online activity, receiving summaries or information about chats.

Analysis
It may be less intuitive than other tools, but it is possible to control both the content visited on the Internet and the use of the device itself.

- Internet browser: Through the browser, it is possible to set filters and prevent certain websites from opening and can even select domains that you want to block.

Analysis
It is very useful to block addresses that contain certain words, specific pages or all those pages that belong to certain categories. Although this tool is very useful to control the use of the Internet, it does not serve to control the device itself.

- APPs: They are suitable for any mobile device, through which minors are usually connected. With these applications it is possible to control the sites they visit, the time spent, avoid downloading other apps, avoid contact with strangers and prevent the disclosure of their data.

Analysis
This is a strong tool which can be chosen from a large number and which is easy to install and use. The only problem is that these apps are usually available for mobile phones and sometimes for tablets, but not always for other devices such as computers or laptops.

The supervision level these apps offer, especially this last group of tools, is very high, which may mean that they are perceived as intrusive. In addition, just as minors have the right to be protected against all forms of abuse that can be found on the network, they also have privacy rights. It is therefore advisable not to make abusive use of these parental control tools, evaluate their use and try to build relationships of trust with children that promote dialogue.

1. Apply knowledge

Exercise SINGLE CHOICE

Associated fine objective:FO_ParentalControl_01_01: You know what technological threats affect minors

Situation: What technological threats affect minors?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Only cyberbullying
- **There are multiple dangers that can affect children, teenagers and youth on the internet (cyberbullying, sexting,...)**
- There is no technological threat that affects minors.

Exercise SINGLE CHOICE

Associated fine objective: FO_ParentalControl_01_02: You can give the definition for the term "parental control"

Situation: What is the definition of the term "parental control"?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **the way in which parents supervise and intervene if necessary, to ensure that the experiences and processes of socialization and personal growth of their children occur adequately and without risks to them.**
- a tool that allows parents to control and / or limit the content to which their children can access the internet from their devices, be they computers, mobiles or tablets.
- a technological threats that could affect minors.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective: FO_ParentalControl_01_03: You can explain what parental control is for.

Situation: What parental control is for?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **to control and/or limit the content to which children can access the internet from their devices, be they computers, mobiles or tablets.**
- to give children the opportunity to surf the internet as they wish.
- to control children social media accounts

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:FO_ParentalControl_01_04: FO_ParentalControl_01_04: You know how technological parental control works.

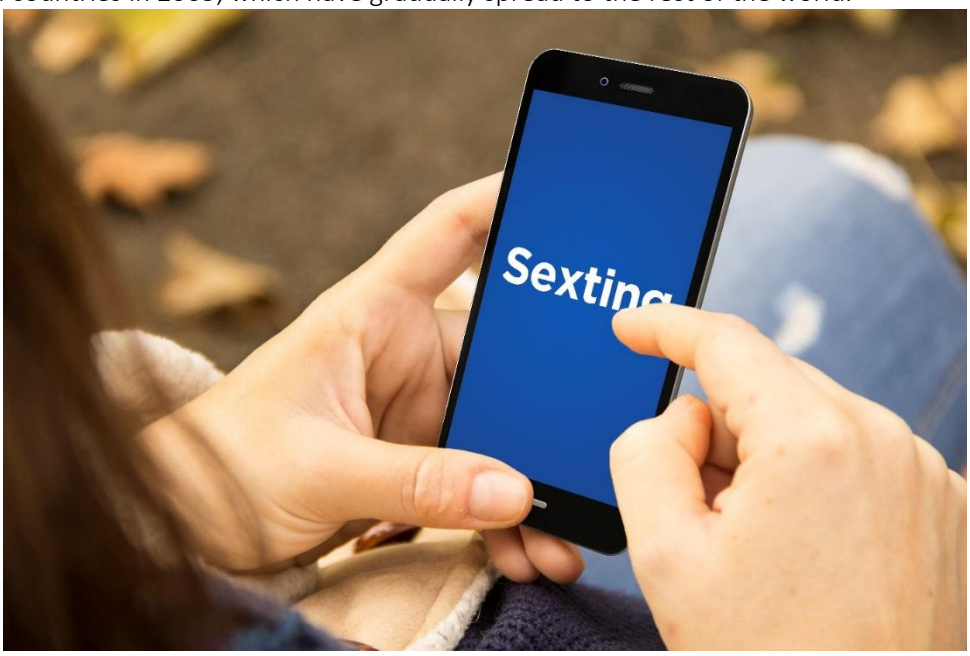
Situation: How does technological parental control works?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Preventing the child from accessing the internet.
- Avoiding using electronic devices at home.
- **The technological parental control can be exercised from different points: outer and DNS servers, the device itself, software, internet browser or APPs.**

2. Build knowledge – What is sexting about?

Sexting consists of sending sexual images or videos, produced by the sender himself, mainly through the mobile phone, or by other technological devices. The term is an anglicism that

comes from uniting the word sex, and texting, sending messages. Its beginnings were in Anglo-Saxon countries in 2005, which have gradually spread to the rest of the world.



To differentiate sexting from grooming it is important to note that in the first case, the images or videos are made by the same sender voluntarily or by another person, but whoever stars in them gives their consent., When minors perform sexting with the harasser deceived, or coerced, it would not be sexting as such, since although in some cases it is voluntary they are being deceived. Sexting differentiates between two actors, those who perform the act of filming, active sexting, or those who receive the images, passive sexting.

Some young people do it as a gift to their partners, as an element of flirting or attracting attention. The risk that this practice contains is that the receiver can send images or broadcast them to have them, or use them to coerce to obtain more images, or other objectives. An inadvertent distribution due to carelessness or error is also possible.

Definition
Sexting …consists of sending (sender) images or videos of sexual content by mobile phone to their pairs (receiver). The person who stars in these videos or images is the same as the sender and they do in voluntarily.

Active sexting is when the person takes photos or videos with suggestive or sexual poses and sends them to another person.
Passive sexting is when people receive photos taken by other people.
Why is sexting thus a potential threat for children and young adults? It is a serious danger on the Internet because, after sending these images, the sender loses all control over them. In this way, this content can reach many more people for various reasons:

- The recipient purposely sends that content to other people, who forward it again endlessly until they reach a very wide audience.
- The main character of the images sends them by mistake to the wrong person, who sends them to other people.
- Someone steals the mobile, tablet or computer of one of those who owns the images, who publishes them on the internet.

- Someone cracks the mobile device or computer of one of those who owns the images, thus sending it to more people, publishing them on the Internet or forwarding them to their protagonist to begin a phase of blackmail or extortion.

Those images can end up in multiple places:

- On the mobile devices of the acquaintances of the protagonist, such as, for example, their own parents.
- Social networks, where you have public access to them.
- Pages of sexual content and/or pornography.
- In the hands of groomers, who see in them their perfect prey so that they can comply with their requests (see grooming).

The consequences for the victim are:

- Humiliation and social lynching for the protagonist of the images.
- The minor faces public insult, affecting first of all his self-esteem, at an age in which their personality is being formed and largely depends on the image that others perveive as the opinion of others is important..
- There are also feelings of helplessness, mainly when the case is told to parents, or educators, or guilt for being in that situation.
- These feelings can lead to deep sadness, anxiety, depression, decreased or increased appetite, or even the most extreme suicide attempts.

Important
The discovery of the distribution of the image leads to the loss of trust in third parties. Relationship problems in the school environment, contributing to a self-imposed isolation to avoid looks, insulting comments, etc.

The prevention of sexting can be carried out by fathers, mothers or guardians, and also by minors themselves.

In the case of parents or guardians:

- They must teach minors that what they share on the internet has its consequences, even if they share it privately with a very close person, this can lead to many problems later.
- Teach them respect for their body and their intimacy. And that no one can force them to do anything that they do not want.
- Locate the computer or make the use of mobile devices as much as possible in places shared with the family.

Minors should avoid sending any kind of photos, but it is known that as they grow up, they start using this functions as well. Even in this transition to become grown-up, it is important to take some measures:

- Do not exchange intimate photographs, much less with strangers.
- Do not post compromised images on social networks or the Internet, these photos later are very difficult to delete and can reach many people.
- If you send an image, try to send it without the possibility of being identified, not showing your face, tattoos, or marks that can easily identify you.
- Do not send images with geolocation coordinates, some mobiles or devices have the option to mark the position where the photo was taken on the image. This can be an added danger in case of spreading the photo or theft of the device, since third parties can know where it was taken and locate the minor.
- If you take a photo and you don't want it to see the light, the best option is to delete it from the device.

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

2. Apply knowledge

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:ParentalControl_02_01: You can give the definition for the term “sexting”

Situation: Sexting consists of…
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Sending threatening sexual messages to a child or a teenager.
- **Sending sexual images or videos, produced by the sender himself.**
- Sending sexual contents such as images or videos produced by the harasser.

Exercise SINGLE CHOICE

Associated fine objective: ParentalControl_02_02: You know the difference between active and passive sexting.

Situation: Active sexting is when…
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **The person takes photos or videos with suggestive or sexual poses and sends them to another person.**
- The harasser asks the other person to send images with suggestive or sexual poses.
- The harraser threatens the other person to send images with suffestive or sexual poses.

Exercise SINGLE CHOICE

Associated fine objective: ParentalControl_02_03 You know the risks associated with the practice and dissemination of sexting.

Situation: After sending these images, the sender loses all control over them because…
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- There are many consequences for the victim.
- The harasser wins power.
- **The content can reach many more people.**

Exercise SINGLE CHOICE

Associated fine objective: ParentalControl_02_04 You can explain three sexting prevention strategies.

Situation: To prevent sexting:

Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **Parents and guardians should teach minors that everything shared on the Internet has its consequences.**
- Parents and guardians should check what minnors do on the Internet.
- Their equals should teach them respect for their bodies.

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

3. Build knowledge – What is grooming about?

Grooming is defined as cyberbullying deliberately carried out by an adult to establish a relationship and emotional control over a minor in order to prepare the ground for sexual abuse.

In some cases, it is performed between minors, but usually with an age difference, where the eldest is usually the harasser.

The objective of grooming is to gain the trust of the minor, to obtain images or videos of sexual content, and even to meet in person. These acts can constitute crimes of corruption, prostitution and sexual abuse of minors.

This type of cyberbullying is closely related to pedophilia, since many also take advantage of the images they have obtained to extort at least by spreading the images if they do not accept the conditions imposed by the aggressor.

Definition
Grooming …adult practices to gain the trust of minors, usually for sexual purposes. This happens on the internet, but sometimes, the harasser tries to establish contact in person.

Usually, "groomers" – harassers – proceed in the following phases:

- Hook: The stalker asks the victim questions in order to get to know them, asks their age and geographic location. Then, try to know their tastes and concerns, to adapt to them, have aspects in common and gain their trust. Here, the stalker does not press with questions that might scare or drive the child away, but rather tries to strengthen ties of friendship with them.
- Loyalty: After making friends with the victim and being friendly, interesting and with many affinities, the stalker makes sure that his new friend wants to continue talking to him. In order to achieve this, he usually talks about topics of mutual interest, sports, music, school, etc., and then continues with family issues, with whom he lives, such as his family, what their parents do, etc.
- Seduction: With all the information and confidence built so far, the harasser is dedicated to seducing, including sexual topics in the talks, and trying to exchange images with the victim. By flattering them and generating a feeling of debt in them, the stalker will get them to fulfill most of his requests.
- Harassment: At this point the harasser already has a close idea of what he can get from the child. He has his private and family information, knows their likes, fears, and

has photos of him or her. The goal now becomes clearer: to establish a sexual relationship, although initially it is virtual. It is possible that at this stage the harasser shows himself as he is, and uses blackmail, threats and manipulation to achieve his goals.

On some occasions, the early stages may begin face-to-face with a person previously known to the child, who subsequently continues the sexual abuse.

In some cases, there may be two more phases:

- Search: In a first phase, thanks to all the information that minors put on unsupervised social networks, in chat rooms, social networks and forums, the harasser searches for his victims taking into account factors such as vulnerability, emotional need, low self-esteem, loneliness and little attention from parents.
- Isolation: An intermediate phase between hooking and seduction, the aggressor takes advantage of the trust he has gained with the child and knowledge, to try to isolate them from friends and family, in order to better control the child, become the closest person and prevent them from contacting someone to tell what is happening to them.

The changes or symptoms that the victim suffers can be divided into four different groups:
Changes in habits in relation to different areas:

- in the use of devices or Internet
- in class attendance, for example poorly excused absence
- abandonment or absence in activities
- ups and downs in study times and in schoolwork performance
- variations in leisure activities
- modification in eating habits
- decreased concentration and maintenance capacity
- special concealment when communicating over the Internet or mobile phone

Changes in mood:

- change of humor
- moments of sadness, apathy or indifference
- unusual attitudes of relaxation and tension, even aggressive reaction
- momentary explosions of aggressiveness

Changes in your relationships:

- strange changes in the group of pairsand/or sudden poverty, absence of friends and social relationships
- lack of defense or exaggerated reaction to alleged jokes or public observations. They may be apparently harmless comments but for the victim it has another meaning.
- fear or opposition when leaving home
- excessive reservations in communication
- changes in their groups of friends, sometimes radical changes
- variations in the relationship with adults, in terms of their frequency and their dependence
- variability of the groups and idols or models or models to follow and imitate
- physical and psychosomatic changes and symptoms, such as:
  - modifications in your body language in the presence of certain people, avoiding contact or closing in on themelves.

- in the occupation of school spaces, fear of recess, and occupation of visible places
- manifestations of disease or frequent ailments
- frequent physical injuries without reasonable explanation,loss or deterioration of garments
- frequent dizziness with uncommon symptoms
- headaches or stomach aches that cause loss of activities or school attendance.

The recommendations to prevent grooming are:

In the family nucleus it is important to promote fluid intra-family communication, thus facilitating the possibility of talking to the children about the Internet, social networks and the potential dangers related to them, making it essential to warn them about the data that they should not provide through from the internet or social networks.

It is also advisable to educate the minor in the safe use of the Internet, tools, services and social networks, with the previous advice, not to provide data, not to accept strangers. The idea is to train them by offering them the necessary knowledge and tools so that they are increasingly autonomous in the use of networks. The supervision and control measures must be adapted to the age of the boy, girl or young person that you want to supervise.

The educational centers can elaborate concrete actions against grooming, counting among the teaching staff with experts who channel and facilitate the information and the technical operation of mechanisms and devices.

They can also adopt methodologies that facilitate the insertion and approach from the curriculum of grooming problems and measures aimed at prevention.

In the case of the minors, they must avoid providing compromising images and information to anyone, or make them accessible to third parties, they must reject sexual or pornographic messages and, in any case, ask for help in new or delicate situations, especially if they involve insecurity or emotional distress.

3. Apply knowledge

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:FO_ParentalControl_03_01: You can give the definition for the term “grooming”.

Situation: Grooming is defined as
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **Cyberbullying deliberately carried out by an adult.**
- Cyberbullying deliberately carried out by an equal.
- Cyberbullying deliberately carried out by a classmate on the Internet.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:FO_ParentalControl_03_02: You know the phases and characteristics of grooming.

Situation: Grooming follows different phases, hook is when...
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- The stalker makes sure that his new friend wants to continue talking to him
- **The stalker asks the victim questions in order to get to know them.**
- The harasser searches for his victimsand their information on the Internet.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:FO_ParentalControl_03_03: You can identify the symptoms of a grooming victim.

Situation: The changes that the victim suffers can be divided into four different areas:
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Habits, mood, hobbies and health.
- Habits, mood, relationships and health.
- **Habits, mood, relationships and psychosomatic.**

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:FO_ParentalControl_03_04: You can explain three grooming prevention strategies.

Situation: In order to prevent minors from suffering grooming, it is advisable:
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- To control what they see, don't let them do it alone and locate the devices in a common area.
- **To have communication, teach them how to use different tools, devices and social networks.**
- Let them use the Internet only when they are autonomous enough.

4. Build knowledge – What is cyberbullying about?

Definition
Cyberbullying Cyberbullying is any kind of bullying that takes place over digital devices such as laptops, tablets or smartphones.

The bully harms the bullied on the Internet, damaging his/her online reputation by spreading messages through the social media such as Facebook, Instagram Twitter, etc., posting in blogs or sending information via e-mail, SMS, smartphone applications like WhatsApp or WeChat.

One of the first steps of the cyberbullying used to be a bully who insults or threats the victim by saying he or she will leak information that will damage his/her reputation. The information sent by the stalker about the harassed may be true, but in this case, it will be leaked on purpose due to the fact of being negative or harmful for the interest of the harassed or it might be directly false. If so, it becomes misinformation.

Example
For instance, a girl receives a message via WhatsApp with a link to a website that includes some pictures of her naked. A stalker asks her to do his homework or he will send this link to her friends and family.

Some of the regular cyberbullying tactics that the stalker will do to the victim are:

- insulting or offending others via internet
- asking the victims to harms their selves or to commit suicide
- threatening
- creating a website or a blog that includes embarrassing information about the victim
- hacking social media profiles, often called ´sockpuppet“
- leaking private data from the victim
- nude photo sharing
- jealousy bullying
- religious, racial or sexual orientation-based harassment

In general, the cyberbully, also known as cyberstalker will be someone close to the cybervictim: a classmate, someone from cultural or sportive activities and most of the times there will be a group of bullies and not only an individual. This kind of behaviour is very painful to the cybervictim because of the next characteristics:

1.Persistency: We live in a 24/7 connected world, where the communication never stops.
2.Permanency: Most of the information published on the Internet remains in the Internet and is public. Moreover, once the cyberbullying has started, the bullies do not use to stop, but they increase their attacks.
3.Hide: The victims do not want to talk about the assaults due to the fear, so it is difficult to notice for the parents, the teachers and other authorities.

Usually, when minors are suffering of cyberbullying harassment, they withdraw into their selves and it affects not only their lives on the Internet, but also to their way of living in the real world.

The cybervictims do not want to keep going to the places where these traumatic experiences are happening to them. They often leave the activities they used to love, they even start skipping their classes pretending to feel sick, what jeopardizes their scholar results, and sometimes they even really get ill due to eating disorders or depressions.

They will increase or decrease the use of the devices and they will become more protective about their privacy, not letting anyone home seeing what they are doing on social media in particular or the Internet in general. Sometimes they even shut their profiles down and create new ones.

In order to prevent cyberbullying, there are some strategies we can deploy:

- Parents and teachers should talk to the children about cyberbullying, reinforcing and rewarding the good behaviour towards others and not only focusing on the bully, but also on the bystanders.
- Adults must seat clear rules about what content must be seen and shared and the amount of time spent in social media. Moreover, they must set the expectations about the right digital behaviour.
- At school teachers can create an anonymous “bullying mail box”, which the students might use to tell they are experiencing this problem and to trigger the cyberbullying protocols.
- Parents and teachers must always keep an eye on any change in mood of the children, no matter how slight it might be.

4. Apply knowledge

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:FO_ParentalControl_04_01: You You can give the definition for the term “cyberbullying”

Situation: Which one of the next answers are correct regarding cyberbullying?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Insulting or threatening others both physical or via internet.
- **Harassing others into the social media, websites, apps or using any other digital channel.**
- Bystanding any negative behaviour into the internet.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective: FO_ParentalControl_04_02: You You can define the roles involved in cyberbullying and its characteristics

Situation: What is the definition of “cybervictim”?
Task: Fill the blanks by typing the term that matches the definition.

- The one who insults, threats or leaks any harmful or mean information about other person.
- **The person who suffers the procces and oftenly withdraw into him/her self.**
- The term “cybervictim” is incorrect.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective: FO_ParentalControl_04_03: You know the consequences of cyberbullying for the stalker and the harassed.

Situation: Which of the next points is not an indicator of being suffering cyberbullying?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **He/she prefers to focus on studying and usually improves his/her grades.**
- Victims usually close their social media profiles and open new ones.

- People suffering cyberbullying change the mood and withdraw into their selfs.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective:FO_ParentalControl_04_04: FO_ParentalControl_01_04: You can explain three cyberbullying prevention strategies.

Situation: How would you prevent cyberbullying?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Calling the police as soon as we have the slightest suspicion.
- Avoiding using electronic devices at home.
- **Setting clar rules about what to do and not to do when using internet.**

5. Build knowledge – What is netholism about? Curiosity, absence of a well based knowledge, free time and a place named Internet where you can find every answer to any question you may have or contact to anyone you mitght want are a breeding ground to spend most of the time in that place. Minors have those characteristics in common.

Internet has expanded teenagers and children world, letting them socialize and express their selves, augmenting their resources for studying, introducing a more peer-to peer-based way of interacting and learning. Those are the bright sides of the Internet, but it also has a dark side, which we cannot ignore.

There are two kinds of addictions: You can get addicted to a substance, but you can also get addicted to a process. This kind of addiction often categorizes as “new addictions”, “not chemical addictions” or “behavioural addictions”. Sometimes, when you spend much time doing something, you can develop an addiction to this process. When you are addicted to spending your time on the Internet, that has a name: Netholism.

Definition
Netholism

Netholism is an internet addiction disorder, also commonly referred to as a compulsive internet use. It does not consist in spending much time on the Internet, but in letting this interfere with daily life because of a dependence to its usage.

This disorder has increased profusely due to the fact of living in a permanently connected society. Whatever you might need, you can find it on the Internet: If you do not find the right size of a shirt in a shop, you can buy it on the Internet; if you do not want to cook, you can order food to be delivered there; if you do not have a sibling to play with on the game console, you can play with a stranger online; if you need to study, all the books, articles and other resources can be accessed via Internet.

In these scenarios, it is very hard to be able to distinguish if a minor is experimenting any kind of Internet Addiction Disorder. Nevertheless, there are some ways of discovering this type of disorder. For doing so, you – as a parent – should ask yourself some questions:

- Is the minor incapable of stopping to use social media when he/she is requested to?
- Is the minor compulsively shopping online?
- Is he or she playing online videogames excessively?
- Is he or she gambling on the Internet?
- Does the minor spend the whole day in front of the computer?
- Does the minor have troubles with social relationships outside the Internet?
- Is she/he experimenting any troubles of not doing her/his homework or are her/his grades decreasing?

If the answer to any of these questions is yes, we should take a deep look on the minor's behaviour because he or she might be experimenting an Internet Addiction Disorder or Netholism.

Nevertheless, it will only be a clue. As we said above, we live in a 24/7 connected world and the barriers between the regular use of the net and the abusive usage of it are slight. So, you will check out whether or not this kind of behaviour has any negative impact on the minor's life. If the minor is not able to prioritize his/her duties and tasks over being online, it is crystal clear he/she has a problem.

Example

It is time for dinner and you call your son to join you at the table, but he is not coming. You call him even three times, but he has the smartphone in his hand, and is not willing to stop what he is doing. Even at the table, he continues checking the stories in his Instagram profile. You take his smartphone and keep it in your pocket and he is literally suffering because he cannot go on with what he was doing.

Another way of finding out if the minor is suffering this disorder is to analyse the amount of time spent using the digital devices, the frequency and the emotional manifestations about not staying tuned. If the minor appears to be depressed, anxious or agitated when he/she is not connected, or if he/she experiments frequent mood swings, netholism could be the reason why.

The Internet Addiction Disorder can also have physical manifestations, such as poor nutrition, pain on the neck, insomnia, dry eyes or poor hygiene.

In order to prevent netholism there are some useful measures to be deployed:

- To limit the amount of time spent using digital devices. Not only by a fixed number of hours, but also by controlling the day time for using them. For instance, never use the computer after dinner.
- Organizing talks at school on the right utilization of the Internet.

- Prioritize family moments over ICTs
- Children should always use the Internet under the supervision of an adult
- Parental control tools (see chapter 1) must be installed in order to avoid the entrance of children and teenagers on gambling or pornographic websites.

5. Apply knowledge

Exercise SINGLE CHOICE

Associated fine objective: FO_ParentalControl_05_01: You can give the definition for the term "netholism".

Situation: Which one is the rightest answer on defining netholism
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Disorder consisting in spending very much time on the internet.
- **Addiction that does not let the victim to live a regular life due to the dependence on the internet usage.**
- A stalker harasses a victim by threatening with leaking nude photos on a website.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective: FO_ ParentalControl_05_02: You can identify alarm signals about abusive internet use.

Situation: Which one of the next are not an alarm signal about abusive internet use"?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **The minor does not want to be oline because he is scared of a bully.**
- The minor plays excessively online video games.
- The minor has troubles when having social relationships outside the internet.

Exercise SINGLE CHOICE

Associated fine objective: FO_ParentalControl_05_03: You know three ways to prevent netholism.

Situation: Which would be the best strategy to prevent abusive use of the internet?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- **to limit the moments of internet using during the days.**
- to give children the opportunity to surf the internet as they wish.
- to control children social media accounts

6. Build knowledge – What is disclosing information about?

Nowadays almost our entire life rests on the Internet. If we get hacked the hacker will find our credit card passwords, will have access to our social media profiles, our e-mail accounts or to our browsing history.

Due to this over exposition, we must take care of our data and avoid the disclosure. Nevertheless, even if we are committed to a responsible use of the internet, we must ensure that minors are as committed as we are, because they use the family devices and their own devices as well.

A wide range of crimes involves the data removal, or the data leakage and teenagers and children are one of the most likely collectives to share their data, because of two main reasons:

1. The digital natives spend more time connected.
2. They do not have a feeling of danger when browsing.

Several techniques can be used to secretly data leak from a digital device. Sometimes the perpetrators hide their intentions by looking as something different than they are. For instance, in the ads, requiring information to visualize the content or asking the passwords to enjoy an online service. But, more often minors share their data because they are not aware of the danger, so a more responsible way of acting on the internet is vitally needed.

Definition
Disclosing information Disclosing means to expose, unintentionally, private information that should not be revealed to other people. It can happen via hacking or because the source does not realize the importance of keeping private data private.

We can say there is disclosure when someone gives his/herpersonal information or places it in a position where they are able to find it out by people who might use it in a harmful way, risking their privacy or security.

This problem has increased profusely due to the improvement and sophistication of the hacking: malware, spyware are only some of the well-known issues. But, as we said above, one of the main problems is that people are willing to share so much information about them. It constitutes a growing problem due to smartphone applications, which ask us access to information such as location, contacts, etc. in order to enjoy their services. This is a change of paradigm that Internet has brought with. On TV they show you content in exchange of your attention. On the Internet they will give you access to applications and services in exchange to your data.

This would not constitute a problem itself if the data revealed were not sensitive. But, does a child know whether the information exposed is sensitive and potentially risky or not? Even adults sometimes

cannot tell this difference. In order to discover if the minors are leaking information, you as parents should ask the minors some questions:

- Which sites do you enter?
- Which applications do you download?
- Has someone asked you to share any personal data to enjoy a service, such as email address or credit card number?

Example
Paul wants to download an application on his smartphone to talk to his friends. Although the app is free, he is required to fill a form that includes the credit card and thecard verification value.

If the apps or the online services ask any information for the proper function of itself which they do not use to ask you to share, or if someone is asking unusual private information, such us your home address, it should be likely to think there would be a risk of disclosing sensitive information.

Sometimes data leakage occurs through the use of a Trojan horse virus. If you have any suspicion of a software, you should never download it. You can suspect of softwares that let you whatch movies or shows in streaming for free, aswell as gaming websites and applications. The best way of acting is to download every service after it has been checked by your parents.

In order to prevent this disclosing, there are some strategies that you as a parent can deploy:

- Tell the minor to not give any personal data without permission
- If your child uses the same device as you: Do not ever keep the passwords or the pin codes on the browser
- Install parental control softwares such as Qustodio, Secure Kids or Parental Click
- Speak to the minors about not to post any photo that let strangers know the exactly address where he/she lives or the school where he/she studies.

- The best prevention tactic is to speak frequently with the minors about the risks of disclosing information and about the importance of a responsible use of the Internet.

6. Apply knowledge

Exercise SINGLE CHOICE

Associated fine objective: FO_ ParentalControl_06_01: You can give the definition of disclosing information.

Situation: Which one is the rightest answer on defining disclosing information.
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

4. Addiction to the digital devices.
5. **Leakage of sensitive information.**
6. Launching fake information on the internet.

Exercise SINGLE CHOICE

Associated fine objective: FO_ ParentalControl_06_02: You can identify when children are leaking information.

Situation: Which one of the next is not an alarm of disclosing information”?

Task: Pick the right options following the multiple-choice principle: Only one answer is true.

7. **The minor asks permission to download a smartphone app.**
8. The minor is required to send the credit card number.
9. The minor posts some pictures at the entrance of the house.

Exercise SINGLE CHOICE

Associated fine objective: FO_ ParentalControl_06_03: You can explain three ways of preventing the information leakage

Situation: Which would be the best strategy to prevent the information leakage?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

10. **To not to keep the passwords and pin codes on the browser.**
11. To let the minors download any app that they want.
12. To spread the personal photos around the social media.

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

Sources

Garaigordobil, M. (2019). Prevención del cyberbullying: variables personales y familiares predictoras de ciberagresión. Retrieved from: https://dialnet.unirioja.es/servlet/articulo?codigo=7041022

Garcia Ganchon, J. O. Seguridad y riesgos: Ciberbullying, grooming y sexting. Retrieved from: http://openaccess.uoc.edu/webapps/o2/handle/10609/72526

Stuttgen, K., McCague, A., Bollinger, J., Dvoskin, R., & Mathews, D. (2020). Whether, when, and how to communicate genetic risk to minors:'I wanted more information but I think they were scared I couldn't handle it'. Journal of Genetic Counseling. Retrieved from: https://onlinelibrary.wiley.com/doi/abs/10.1002/jgc4.1314

Villanueva-Blasco, V. J., & Serrano-Bernal, S. (2019). Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género. Revista de Psicología y Educación, 14(1), 16-26. Retrieved from:https://www.almendron.com/tribuna/wp-content/uploads/2020/05/patron-de-uso-de-internet.pdf

1. Save knowledge

Summary

This unit focusses on the importance of parental control to protect children and adolescents from dangerous situations using internet or technological devices.

Since we are in a changing world where technology evolves day by day, the dangers minors have always faced can come through new routes. These risks can also spread and magnify easily through the Internet.

In order to carry out the task of keeping minors safe while they interact and expand their circle, it is necessary to know the risks and the ways to avoid them. For this purpose, it is important to set the ways in which dangers could reach the youngest ones (social networks, games, video platforms, etc) and the available tools to stop or detect them.

Having exposed the different ways in which dangers can reach children and teenagers and the tools and functions to keep them under control, it becomes necessary to specify these risks and their consequences. Some of the dangers that minors face are sexting, grooming, cyberbullying, netholism and, disclosing information. These dangers should be understood to deal with them or even to detect them.

Some of these consequences can directly affect minors' emotional and even physical health. If we pay attention, there are visible effects that can drive as to the root of the problem to take action.

However, the best option, when possible, would be preventing situations such as sexting, grooming, cyberbullying, netholism, and data disclosure instead of dealing with them. In order to do so, ways of exercising parental control on the Internet and technological devices and some tools will be exposed. It will also be possible to find some tips to keep minors away from each of the dangers mentioned above.