Content Unit

[Protection against inappropriate content]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: bit cz training
Last processing date: 24.6.2020

Funded by the
Erasmus+ Programme
of the European Union

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

Protection against inappropriate content

First introduction

The internet in this digital period offers to explore many ways of a virtual world without the constraints of the actual real world. Content on the internet is not broken into age or developmentally appropriate areas. And that is the problem! Some content may be illegal, inappropriate, offensive or unsuitable for some age groups. Without supervision and guidance, anyone, even a little child, can find content that is disturbing, explicit or inappropriate. Many disturbing websites are not 'illegal' which means that no one monitors and manages them. Seeing inappropriate online content accidentally can have a traumatic effect especially on your children. The example of inappropriate content could be: promoting hate based on race, religion, disability, sexual preference, violent extremism, sexually explicit content, real or simulated violence. As a parent you need to protect and guide your children during their first steps on the internet and educate them so they become responsible and independent Internet users.

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

After learning this content unit, you will know what is inappropriate content, what it includes and how to protect yourself against it.
Further, you will learn about methods of spreading inappropriate content and about the impact on everyday life.

Overview of learning objectives and competences

In LO_ Protection against inappropriate content _O1 you will know all the important aspects that are hidden under inappropriate content and how to protect yourself against it.
In LO_ Protection against inappropriate content _O2 you will see how inappropriate content affects children and adults as well as their private life and work.
In LO_ Protection against inappropriate content _O3 you will see internet sources and measures useful to provide information about inappropriate content and how to behave safely on the internet.

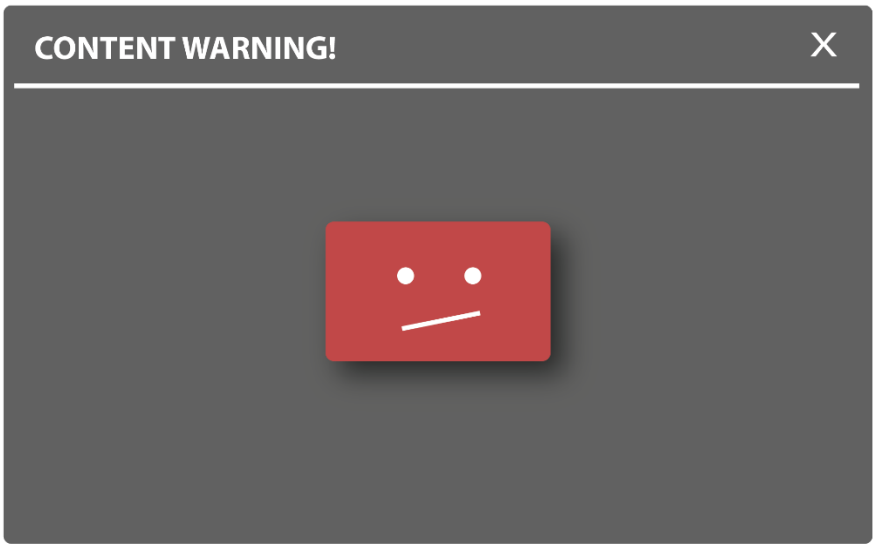
Learning objectives	Fine objectives
LO_ Protection against inappropriate content_01: You know the characterization of inappropriate content.	FO_ You know the characterization of inappropriate content.01_01: You can name the types of inappropriate content.

	FO_ You know the characterization of inappropriate content.01_02: You can name the methods of spreading inappropriate content and obtaining sensitive information. FO_ You know the characterization of inappropriate content_01_03: You can name the ways of rating and reviewing the content appropriateness. FO_ You know the characterization of inappropriate content_01_04: You can recognize unsafety content on the internet.
LO_ Protection against inappropriate content_02: You know the threats of abusing sensitive information and their impact.	FO_ You know the threats of abusing sensitive information and their impact.02_01: You can describe the impact of spreading inappropriate content on children. FO_ You know the threats of abusing sensitive information and their impact.02_02: You can describe the impact of spreading inappropriate content in your private life as well as in your work. FO_ You know the threats of abusing sensitive information and their impact.02_02: You can characterize the target groups that could be victims of aiming for inappropriate content.
LO_ Protection against inappropriate content_03: You know how to protect yourself against inappropriate content.	FO_01: You can manage and report abuse, spam, or inappropriate content on social media website. FO_02: You can find the contacts and sources useful for helping to stay safe, protect from abuse. FO_03: You can explain how to block pages with inappropriate content. FO_04: You can name the technical approaches how to prevent from capturing sensitive information. FO_05: You can name the reasons why some personal information should not be published online. FO_06: You can understand EU legislative measure against spreading inappropriate content.

1. What is inappropriate content?

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

Inappropriate content is a term used to capture a wide and ever-increasing number of different types of problematic content online.



Generally inappropriate content is anything that violates the rights of the child as defined by the Convention on the Rights of the Child and everything that violates human rights as defined by the Charter of Fundamental Rights and Freedoms, in particular the right to life, privacy, information, protection and the right to participate in society, to be protected from abuse and violence. It can be anything from hate speech to images of self-harm or pro-ana websites. Inappropriate content might include the following topics:

- Pornography
- Violence, Extremist behavior
- Dangerous products
- Racism or Hate
- Pro-Ana sites
- Sites with extremist content

To display the characteristics of these subtopics, we will have a look at them in detail:

Pornography

Pornography is described as an explicit description or image intended to stimulate sexual feelings. However, pornography may or may not be obscene; as long as it is argued that the work has literary, artistic, political, or scientific value. But a lack of consensus hinders objective attempts to define pornography by one definition.

Definition
Definitions of pornography vary from time to time and place to place: Something defined as pornographic a few years ago may now be considered erotic. Internet pornography is any pornography that is accessible over the Internet, primarily via websites, peer-to-peer file sharing, or Usenet newsgroups. The availability of widespread public access to the World Wide Web in late 1990s led to the growth of Internet pornography.

Here are some examples of internet pornography:

- Depictions of nudity in which the subject is nude or minimally clothed, and where the clothing would not be acceptable in an appropriate public context.

- Depictions, animations or illustrations of sex acts or sexually suggestive poses.
- Content that depicts sexual aids and fetishes.
- Content that is lewd or profane.
- Content that depicts, describes or encourages bestiality.
- Apps that promote sex-related entertainment, escort services or other services that may be interpreted as providing sexual acts in exchange for compensation.

Violence, Extremist behavior

Violence is not just the domain of computer games or movies. The Internet also gives it a lot of space, especially video-sharing portals, where brutal live-action videos appear as well as real attacks or real events with a tragic end. There are even specialized portals that focus on collecting links to brutal videos and photos. It is difficult to prevent violent content from being presented on the Internet, as most of the time there is no violation of any law.

Common violent content on the Internet refers to graphic depictions or descriptions of realistic violence or violent threats to any person or animal. We may also come across apps that include manifestations of violence. These apps can promote self-harm, suicide, eating disorders or at first glance harmless games, or other acts where serious injury or death may result.

In extreme cases, you can meet with content related to terrorism, such as content that promotes terrorist acts, incites violence or celebrates terrorist attacks.

Remember
Content related to terrorism or violence can also serve for an educational, documentary, scientific or artistic purpose. For that type of purpose it is necessary carefully consider the use of the content and consistently explain the noxiousness of that behaviour

Dangerous products

Many people do not realize that the Internet is a means that can offer and facilitate the sale of explosives, firearms, ammunition or certain firearms accessories. Other possibilities include components serving for the manufacture of explosives, firearms, ammunition, restricted firearm accessories or other weapons and instructions on how to convert a firearm to automatic, or simulated automatic, firing capabilities.

Darknet market or cryptomarket is an illegal commercial website on a special non-public website called darknet, which can only be accessed with specific software, configurations, or authorization. It primarily functions as a black market, for the sale or brokering of transactions involving drugs, cyber-weapons, weapons, counterfeit money, stolen credit card data, counterfeit documents, illicit drugs, steroids and other illegal goods, but also legal goods.

Racism or hate

Promotion or incitation of hatred against individuals or groups based on race or ethnic origin, religion, disability, age, nationality, veteran status, sexual orientation, gender, gender identity, or any other characteristic is also a common type of inappropriate content that is associated with systemic discrimination or marginalisation. Assertions intended are to prove that these individuals or groups are inhuman, inferior or worthy of being hated. These activities include negative characteristics (e.g. malicious, corrupt, evil, etc.), statements that the group is a threat or speech trying to encourage others to believe that people should be hated or discriminated because they are a member of some group.

The Internet offers unlimited space for publishing almost any content, text, video, photo or music. Besides, anyone - be it an individual or a group of people, an organization, or a business – can get their

Internet presence through a blog, website or social profile. Despite all efforts to regulate, the inappropriate content , the people always finding the new opportunities and ways how to get it on the Internet. The common ways of spreading include:

Pro-ana sites

Pro-ana sites, blogs, forums, and social networking groups are the voice of a movement that understands anorexia as a lifestyle, not as a disease. Anorexics do not see anything wrong with their lifestyle, but they perceive the resistance of their surroundings, so they gather and support each other. By enhancing their own pathological experience and behavior on websites and social networks, they ensure a sense of really positive feedback. Opinions on pro-ana sites vary - the first part argues that pro-ana exists as a safe environment for anorexic persons to discuss their illness and thus support those who opt for recovery, the second part uses pro-ana sites to support their view that anorexia nervosa is not a disease but a lifestyle that should be respected by doctors and family.

Sites with extremist content

Sites with extremist content often seem innocent at first glance: they provide attractive information such as historical events, but facts are distorted and refer to other sources of information already manipulated by a shifted perception of the world. Similarly, extremists make use of, for example, music group presentations, in whose texts published on the website there is usually hidden extremist content.

Social network

As in newspapers or television, it is not allowed to distribute illegal content – such as child pornography or violence – on the Internet. Despite all efforts to regulate, this content appears on the Internet. Besides, the Internet provides space for the distribution of legal but inappropriate content such as simple pornography or violent content that may interfere with the healthy development of children.
For online communication, it is becoming increasingly common to voluntarily send sexually suggestive messages and intimate pictures or videos. And with the boom of social networks, it is even easier to distribute such content.

Sometimes it is very difficult to tell what is inappropriate content and what is not.

Pornography is often confused with the term erotica.

What is the difference?

What constitutes pornography and erotica varies in the change between groups and also between individuals. It is also likely to vary with the time - what was considered pornographic perhaps in the early 1900s may now be considered erotic.
The criteria used for distinguishing between the erotic and pornographic is very steeped in personal moral, aesthetic, and religious values. Even though many people regard these two orientations to human sexuality as overlapping, there is existing the significant difference between them. Erotic unlike pornography doesn't appeal exclusively to our senses or carnal appetites, it also engages our aesthetic sense, our judgment about how the figure illustrates an ideal of human beauty. Erotic is rather an artistic and aesthetic matter, pornography is more oriented towards the instinctive satisfaction of sexual needs.

Classification of pornography in terms of psychology:

- soft = everything erotic, from an artistic act to a hint of a sexual act
- hard = direct depiction of sexual act, including details of genitals, their irritation, erection, penetration, ejaculation
- deviant = direct depiction of sexual deviations and practices that do not occur in a common and generally accepted sexual life in a given culture (society) - child, sadomasochistic, etc.

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

Pornography vs child pornography
Not every depiction of the naked body is pornography. For this to be the case, it must be such a work (photographic, computer, written or other) whose purpose is to induce or increase sexual arousal (pornography is not, for example, the depiction of genital organs in a biology textbook). Therefore, the determination of whether pornography is already based on the prevailing moral feeling. Child pornography is one that depicts or otherwise uses a child or a person who appears to be a child. Currently, these include images of children depicting the positions of actual or feigned sexual intercourse (in extreme cases it may not even be directly visible to the exposed genital organs) or images of the naked children in positions challenging to present the genital organs. European and national laws prohibits the production, distribution, importation, reception, or possession of any image of child pornography. A violation of child pornography laws is a serious crime, and convicted offenders face fines severe statutory penalties.

1.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_ You know the characterization of inappropriate content.01_01: You can name the types of inappropriate content..

Situation: What topics can we consider as the inappropriate content ?
Task: Pick the right options following the multiple-choice principle: More answers could be true.

- Art with erotic pictures
- Websites with Racism or hate
- Action movies generally
- Sale of Dangerous products
- Documentary war film with the extrem violence

2. How to recognize the websites with inappropriate content?

There are already several institutions that oversee disposition of online content. It is good to be able to distinguish the quality and credibility of information and to know how to deal with threatening material.

Common Sense Media

Common Sense Media is a movie, series, book, app and other content rating company which recommends the appropriate age for that content. It also offers users the opportunity to evaluate.

Kids-In-Mind

Kids-In-Mind describes what children will see in a film, but does not recommend which age group it is suitable for.

Other options

IMDb Movie Database provides useful information. In the movie details, search for Parents Guide and click the View content advisory link. You will be taken to the detailed information page. You can also find age recommendations based on country-specific rules.

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

There are also several ways that you can work out whether a piece of content is suitable for your child. Many platforms use a type of rating to advise on the level of violence and explicit content that a piece of media contains.

Here are just some things you can watch out to help you make an informed choice on whether an app, website or piece of content is suitable:

Online music videos ratings

The ratings appear on the two biggest video sharing platforms VEVO and YouTube. On YouTube, you'll see the 'Partner Rating' label on the video below the video which will show whether the video is suitable for age from12, 15, or 18 (PG 12, 15 or 18). On VEVO you'll see the rating symbol on the top left-hand corner of the video player when the video loads. You can also click on the 'i' for more information about the rating.

Online gaming PEGI ratings

Pan European Game Information or PEGI are used to advise on which video games are suitable for older or younger teens or adults only due to the type of content they have. PEGI ratings were introduced in 2003 and range from PEGI! (Parental Guidance Recommended), PEGI 3, PEGI 7, PEGI 12, PEGI 16 and PEGI 18. The number relates to the age that the game is appropriate for. So, if a game has a PEGI 7 rating, it is suitable for children 7 and over. These ratings are legally enforceable so it is illegal to sell a PEGI 18 game to a child. Also, these ratings do not relate to the level of difficulty of the game, just to the level of appropriate content.

On-demand platforms

On platforms like Netflix, BBC iPlayer and Amazon Prime, you'll see age ratings displayed across the content they have on offer. These may differ from platforms but the rating will always advise if something is for a 'mature' audience or specify if the content 'contains strong language'.

Social media platforms minimum age of use

Most social media platform's terms and conditions advise that children should be 13 and over to use the platforms. The reason for this minimum age is not to do with the fact that the content on the platform is only suitable for 13 and over but due to COPPA (Children's Online Privacy Act) which is a US law passed to protect the privacy of under 13s.

Understanding App age ratings

Both the Google Play Store and Apple app store use app ratings to highlight the level of sexual content, swearing, mature themes and substance abuse an app may contain.

Accessibility abbreviations you may encounter on the Internet (source: Motion picture Association rating):

- G: Children's film, completely safe
- PG: Parents should consider letting children watch
- PG-13: Children under 13 years with parents only

- R: Under 17 years only with an escort
- NC-17: not suitable for younger of 18 years

Remember
Parental Controls, Privacy Settings and various ratings are useful tools to help minimise the risks your children may face, but they are not 100% effective. It's really important to teach your child skills like critical thinking and resilience, so they know what do if they encounter risk. Always encourage them to talk to you about anything they find upsetting online.

As soon as your child starts to use the internet you should begin to talk about what they might find there. Help them understand that sometimes they may come across things that they'd prefer not to see, or that you would prefer they didn't see. Try to have these conversations regularly.

- The recommended measures how to avoid the inappropropriate content:
- Explain age limits and age-inappropriate sites
- Talk to other parents and the school
- Agree ground rules
- Be calm and reassuring
- Age verification on commercial porn sites
- Encourage critical thinking
- Talk about what is fake and what is real
- Talk about positive ways how to use tech

Remember
It's important to keep the conversation going and take an interest in what your child is doing online.

2.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_ You know the characterization of inappropriate content.01_02: You can name the methods of spreading inappropriate content and obtaining sensitive information.

Situation: What content is discussed on pro-ana sites?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- placing obscene materials
- collecting links to brutal videos and photos
- promoting self-harm, suicide or brutal games
- **talking about anorexia**

3. What is inappropriate content for my child?

Without guidance, young people have access to a virtually limitless world, so parents should be aware of the risks. The Internet is open to anyone to post and create content so sometimes your children may see things they wish they hadn't or access sites that are inappropriate for their age. Inappropriate can

mean different things to different people, from swear words to pornographic images or videos, and what is inappropriate for your child will also change as they grow and develop.
There is a range of things online that might upset children and affect what should be a healthy online experience. It's important to remember that inappropriate content online includes pornographic content, but could also include other content such as race hate, pro-eating disorders or gambling sites.

What content is inappropriate for a child?
Inappropriate content includes in most cases information or images that upset child or information that might lead or tempt your child into unlawful or dangerous behaviour. This could be:

- Pornographic material
- Content containing swearing
- Sites that encourage vandalism, crime, terrorism, racism, eating disorders, self-harm or even suicide
- Pictures, videos or games which show images of violence or cruelty to other people or animals
- Gambling sites
- Unmoderated chat rooms – where there's no one supervising the conversation and barring unsuitable comments
- Sexism or sites that portray females in very traditional roles that do not reflect contemporary values and expectations

Generally almost all persons are affected by the inappropriate content and we can divide them to the several categories to define the specific issues of the protection :

- Pre-school (0 – 5 years)
- Younger school-age (6-11 years)
- Older school-age (12-15 years)
- Youth (15-18 years)
- adults

Pre-school
More and more pre-schoolers are using their parents' computers, smartphones or tablets to play games, use apps, and watch their favourite TV shows. There are simple things you can do to make sure they're

using the internet safely. It is necessary to build up the good relationship to the correct content by exploring together, installing the parental controls, using the passwords not to allow the admission and set the boundaries/rules to be online.

Younger school-age

Early use of digital technology has been shown to improve language skills and promote children's social development and creativity. But it's not without risks for young children, who may come across inappropriate content or begin to copy what older children do online. You can use the same issues as for pre-school children and to complement it by using the airplane mode (not allow to communicate with other people through your device), talk to any older children about what they're doing online and what they show to younger children and to monitore the age ratings what is suitable for that age.

Older school-age

Primary school pupils are the riskiest group in terms of the massive increase in the use of modern technology without relevant instruction and control, easily abusive naivety, defiance of authority and the search for their own identity, which, if not satisfactory in the real world, runs into the virtual world. It is common for a given age group that their virtual life is subject to minimal, superficial or no parental control, often being more computer literate than parents themselves, who often perceive modern technology hostile and let the children use it to have a relax for themselves. Therefore, a large proportion of young users have developed the feeling that they can do anything in the virtual world that they like without the sense of responsibility and respect of other users.

Youth

Students of secondary schools and vocational schools are specific for their deeper use of modern technologies, especially the Internet and social networks and the dangers arising from them. Your child should set privacy settings on most social networking sites so that only close friends can search for them, tag them in a photograph or share what they've posted. Let them know that anything they upload, email or message could stay around forever online. Remind them they should only do things online that they wouldn't mind you, their teacher or a future employer seeing. Get them to think about creating a positive digital footprint. Remind them how important it is not to give in to peer pressure to send inappropriate comments or images. For that target group is the most important your trust. You have to be interested in their needs, to speak with them and be rather the friend than parent. Share your content with them and try to motivate them to share their content with you.

Adults

Adult content may also be affected by inappropriate online content. Many websites contain viruses. These are most often placed on pages with inappropriate content. In most cases, this is a download by mistake of a computer virus spread across pornographic content sites. These sites are very appealing to cybercriminals because they have a large number of users. Moreover, they are often reluctant to report a cyber-attack or infection to their device because they are embarrassed if they are found to be from pornographic sites. The most common digital diseases that users can download visiting websites with inappropriate content to their device include trojans, clickjacking, tinder bots, cat-phishing, ransomware, worms, pornware, or spyware.

3.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_You know the threats of abusing sensitive information and their impact.02_02: You can characterize the target groups that could be victims of aiming for inappropriate content.

Situation: What group of people is most vulnerable against inappropriate content?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- old people
- **children between 12-18 years**
- all children under 15 years
- all children over 15 years

4. How can I protect myself and my children from inappropriate content?

Tools like parental controls can help to protect your children from accessing inappropriate content, but you can't check everything they see on the internet. You need to help them avoid unsuitable content, and cope with it if they see it. The first step is to talk to them about it.

Most of these disturbing websites are not 'illegal' which means that they will remain online and it is up to a parent to monitor and manage. You would not feel safe allowing your child to wander aimlessly through a large city, alone and in the middle of the night so remember that the internet is like a large city, full of good and bad and a place that a child needs to be supervised.

What can I do when I recognize the websites with innapropriate content?

- To inform the appropriate administrator directly in application (web browser, social networks etc.)
- To inform the police or other relevant institutions
- To use the software tools to block the inappropriate content (parental control)
- To speak with the children about that topic

It is possible to inform the application manager about the innapropriate content in common applications (Google, Facebook etc.). Usually you can find the botton in the application settings.

You can also inform the police office about the inappropriate content by the detailed specification of the source.

Parental controls are software or device-specific options that allow parents to monitor their child's internet use. They prevent children from accessing inappropriate or unsuitable content online. They can be implemented within your internet service provider, search engines, video streaming sites and more. The most often tools oft he parental control on the Internet is:

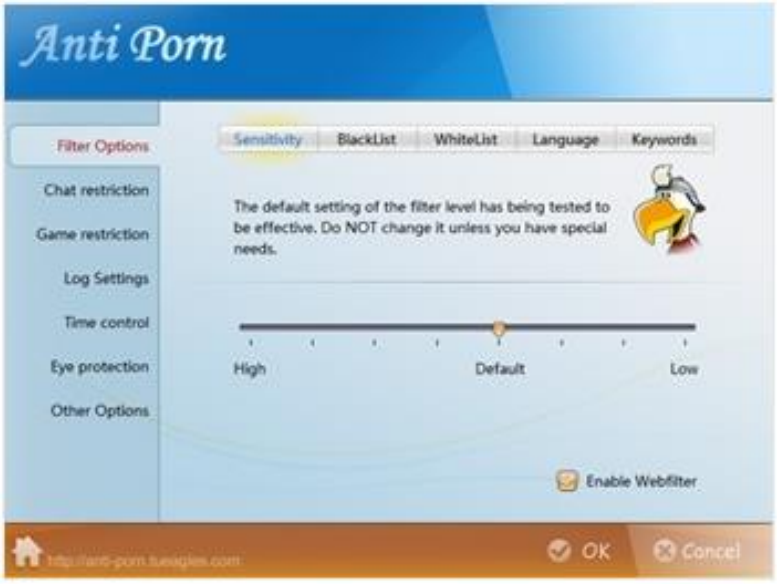
- Set up the parental controls for your network on router
- To use the applications monitoring the child‘ s internet time
- Restrict internet access on my wifi
- Put the parental control on web browsers

If you are trying to avoid visiting problematic sites from your computer not only for children, but also for employees - some topics can distract them from work - typically those with pornography, extremist issues, , you can use several types of protection methods.

What program, filter, or add-on is best for restricting access to these inappropriate sites?

Anti-Porn

One of the best known and most widely used programs to prohibit pornography visits to the web. This is mainly due to its easy maneuverability and easy adjustability. The application automatically recognizes and marks content as erotic and immediately forbids access to that side. It also has a database of several thousand malicious websites, which is regularly updated.



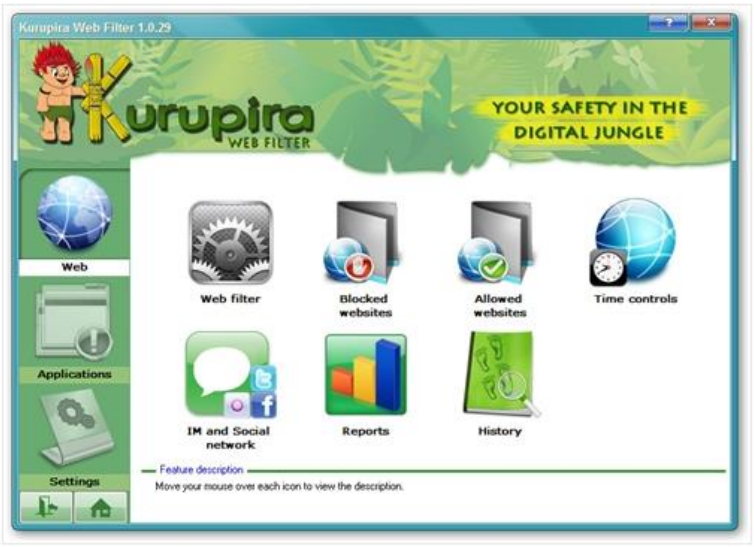
K9 Web Protection

Another filter program to protect against the pitfalls of the Internet. Both a malware protector and an inappropriate content filter can work. It is free and can be used on both Windows and Mac OS X. Also, this program is easy to set up and operate. Malicious sites are categorized by type for pornographic, social networking, violent content, etc.

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

Kurupira Web Filter

Not well known and widespread program, but it can handle its work very well, yet in a pleasant and beginner-oriented environment. The advantage is also a free application license. To access the program, you fill in a password so that only knowledgeable passwords can set filters.



iWebFilter

The application contains a wide database of problematic pages, words, and content, and of course, the user can extend it. Blocking can be set for both web browsers, Instant Messengers (IM) and email clients and other applications. There is also an internet access schedule, data transfer limit and detailed log of events.

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

In the event of encountering objectionable content, you should not continue watching it, but turn off the screen or leave the screen. The adult should not reprimand the child for browsing in inappropriate places on the Internet. It is not for what is displayed on the Internet. If you find that your child is watching pornography, violence, etc. intentionally, you should think about the cause. It is necessary to take into account age and event or seek professional advice, e.g. in the relevant pedagogical-psychological counseling center.

Insafe and INHOPE work together through a network of Safer Internet Centres (SICs) across Europe – typically comprising an awareness centre, helpline, hotline and youth panel Hotlines, dedicated to the removal of illegal online content), operate Safer Internet Centres (SICs) in 30 European countries in the drive to keep children and young people safe online. Through a range of services, SICs respond to the latest online issues, helping to promote the many opportunities the online world offers, while also addressing the challenges.

How to report inappropriate content?
If you or your child come across any inappropriate content which incites violence or hatred, here is what you can do:

- In case of illegal content (breaking the law) you should mainly contact the police
- Contact the organizations/institutions focused on internet safety (f.e. SICs: https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope) to help you with the content removal/blocking
- Report to the administrator of the page/platform
- Change the settings in your computer
- Contact the experts to help your child with the traumatic situation
- Talk with your child
- Keep calm

Here are quick video how-to guides to set the right settings on the most popular platforms and other things you can do:

Facebook Privacy Checker
https://www.youtube.com/watch?v=wN3jz2Mv_ME&feature=emb_title

YouTube Restricted Mode

https://www.youtube.com/watch?v=XuXnatkASTQ&feature=emb_title

Google SafeSearch
https://www.youtube.com/watch?v=LK-MIwjQz20&feature=emb_title

Security and spyware

Some computers especially in the public places (library, coffee-shops, schools etc.) might have some monitoring software that can capture the screen and thereby poses a threat to sensitive information on the screen. These PC surveillance tools can monitor all kinds of activity on a computer. Anti-virus software and firewalls do not fully protect the system against the majority of spyware and privacy threats. Spyware is commonly bundled with software downloads, attached to e-mails, or transmitted through networks so it appears to be legitimate software, but once installed it can be nearly impossible to detect and remove it without the help of a dedicated spyware removal tool. Spyware protection and prevention are essential to defend privacy from prying eyes and virtual trespassers. That measures can also be installed to the private computers to protect you and your children from the inappropriate content by monitoring the whole activity online. The examples of those tools you can find in the text above.

Here are some quick tips for identifying dodgy sites and apps:

- Check that the URL for a website is the main URL you normally use to access that site.
- Be wary of any emails from people you don't know. If in doubt don't click on links or open attachments in emails.
- Check that the branding is accurate — that it appears the same across all platforms — and the logo is not blurred.
- Are there typos on the website or in emails asking you to log in and update your details? If so, then it's likely to be a scam.
- Check your app store for reviews of apps before you download them. If there are lots of users and good reviews, it's unlikely to be a scam. If there aren't any reviews, do some more online research — scams usually get identified fairly quickly and people often post online about them.
- Is an app asking you to input lots of personal information or provide your login details for any social media accounts? Then, it's likely to be a scam.

Personal information

The other issue concerning the inappropriate content should be also publishing of your personal information. Everybody can see and download whatever you publish online and use it in other context or misuse the information.

The most important type of information to keep private is personally identifiable information (PII).

Definition
According to the U.S. General Services Administration, PII is "Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."

Some examples of PII are:

- Names: Your full name, your maiden name, and your mother's maiden name
- Personal ID numbers: Your social security number, driver's license number, passport number, patient ID number, taxpayer ID number, credit account number, or financial account number
- Addresses: Your street address and email address
- Biometrics: Retina scans, fingerprints, facial geometry, or voice signatures
- Vehicle ID or title numbers
- Phone numbers
- Technology asset information: Media Access Control (MAC) or Internet Protocol (IP) addresses that are tied to a certain individual

Why you should keep your personal information private? Securing your personal information can help you to prevent identity theft, protect your financial information, avoid being robbed, protect your employability and business's reputation and much more.

Here are some tips so you can keep your accounts secure and stay in control of your online privacy. You can also read more about how to protect your identity.

- Do a privacy check-up by going through the settings for all your social media accounts
- Set strong passwords and update your old ones
- Don't share your passwords
- Make sure you download and install new operating systems and software on your phone, tablet or computer as soon as they become available.
- Don't add people on social media that you haven't met offline
- When websites or apps ask for your personal information, double-check they are legit

The European Commission adopted a recommendation on measures to effectively tackle illegal content online. Issues such as incitement to terrorism, illegal hate speech, or child sexual abuse material, as well as infringements of Intellectual Property rights and consumer protection online, need a strong coordinated EU-wide approach. The approach is fully aligned and consistent with the Copyright Directive, including widely debated aspects of the liability of online platforms. It is also fully consistent with the revision of the Audio-Visual Media Directive.

Online platforms need to be more responsible for content governance. The recommendation proposes a common approach to quickly and proactively detect, remove and prevent the reappearance of content online:

- Clearer 'notice and action' procedures
- More efficient tools and proactive technologies
- Stronger safeguards to ensure fundamental rights
- Special attention to small companies
- Closer cooperation with authorities

4.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_ You know the role of cybercrime on the internet.03_05: You can name the personal information that should not be published online

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

Situation: What are the basic ways to prevent spreading inappropriate content?
Task: Pick the right options following the multiple-choice principle: More answers could be true.

- **Don't send your photo to anyone you don't know.**
- **Keep passwords secret and do not disclose them to a close friend.**
- **Do not open the attachment of a message that came from an unknown address.**
- Don't visit any social website.

Sources

Internet matters.org: https://www.internetmatters.org/issues/inappropriate-content/learn-about-it/#age-ratings

CNET.com: https://download.cnet.com/Anti-Porn/3000-27064_4-10207334.html

K9 Web Protection: https://www.downloadsource.net/1771222/k9-web-protection/

Soft free download (Soft 32): https://kurupira-web-filter-and-parental-control.soft32.com/

Softpedia: https://www.softpedia.com/get/Internet/Other-Internet-Related/iWebFilter.shtml

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

Save knowledge

Summary

The forms of objectionable content are rich. The most common include

- Pornography
- Violence, Extremist behavior
- Dangerous products
- Racism or Hate
- Pro-Ana sites
- Sites with extremist content

Often the content is undesirable and harmful, but it may not be illegal. This depends on how to load them, respectively how to prevent its accessibility. However, both illegal and legal harmful content can similarly have an undesirable impact on those who encounter it.

In general, it is advisable to contact the police with illegal acts. However, it is sometimes essential, above all, to quickly prevent the distribution of such content, and it is possible to turn elsewhere for that purpose. If you encounter illegal pornography or an extremist site, report it to the Police.
First of all, children (depending on their age) shouldn't meet dangerous content at all. For example, **filters in the Internet browser** can be helpful (for example, it is possible to disable the display of a page containing the term "porn", etc.).

Parental controls are software or device-specific options that allow parents to monitor their child's internet use. They prevent children from accessing inappropriate or unsuitable content online. They can be implemented within your internet service provider, search engines, video streaming sites and more. The most often tools oft he parental control on the Internet is:

- Set up the parental controls for your network on router
- To use the applications monitoring the child‘ s internet time
- Restrict internet access on wifi
- Put the parental control on web browsers

The most important protection against the inappropriate content is the **discussion and care for our children**, to know what they do and to be interested in their needs and hobbies. We can have the helpful tools for protection as the laws, parental controls, software settings, supporting institutions, but the key is the trust between you and the child.