eSafety Label
for a safer school

Tips&Advice

SECURITY POLICIES for SAFER INTERNET

Tips for Students, Parents and Teachers

ΙΔΡΥΜΑ ΚΡΑΤΙΚΩΝ ΥΠΟΤΡΟΦΙΩΝ IKY
Erasmus+
2017-1-EL01-KA201-036242

CTI "DIOPHANTUS" Computer Technology Institute & Press
European Schoolnet
NCBI
HELLENIC REPUBLIC
National and Kapodistrian University of Athens
REPÚBLICA PORTUGUESA
EDUCAÇÃO
direção-geral educação

Cyberbullying

Students

- Stop communicating with the bully immediately
- Do not respond and do not retaliate
- Do not promote intimidating or threatening messages
- Keep evidence of bullying (photos, dialogues, messages, etc.)
- Inform your parent or another adult you trust that you are being bullied

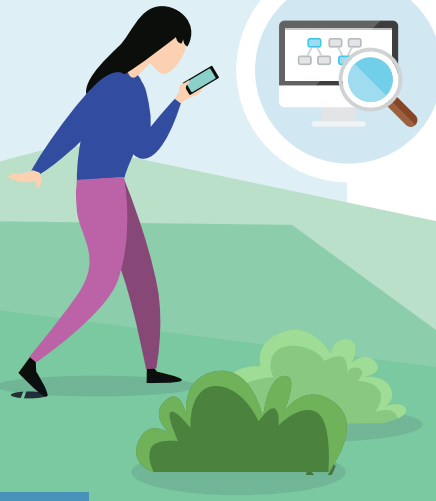
Parents

- Make sure to establish a relationship of trust and cooperation with your children
- Check for a potential change in your children's behavior that may be a sign of bullying
- Help your children to filter emails, restrict access to their blogs, remove bullies from their contact lists
- Try to limit the incident as soon as possible
- Inform the school about the incident and collaborate with the school staff
- Offer your children the proper support as soon as possible, ensuring that their physical and mental health is not directly at risk

Teachers

- In case you know the offender, take measures to change his/her attitude and behaviour
- Proceed to seizure of digital devices by acting in accordance with law and school regulations
- Inform other staff members, parents and carers, as appropriate
- Provide support to the victim so that he/she feels safe and confident that such incident will not happen again and that the school community has been taught from it
- Record and substantiate the bullying incident

Digital footprint



Students

- Do not reveal everything on the internet about yourself
- Do not post messages or comments with negative content
- Avoid publishing on the internet if you are in a bad psychological condition (i.e., angry, irritated, sad), because you may regret it later on
- Do not post photos while you are away from home
- Delete social media accounts which you no longer use
- Ensure that the information you see and share on the internet is legal and positive for you and others

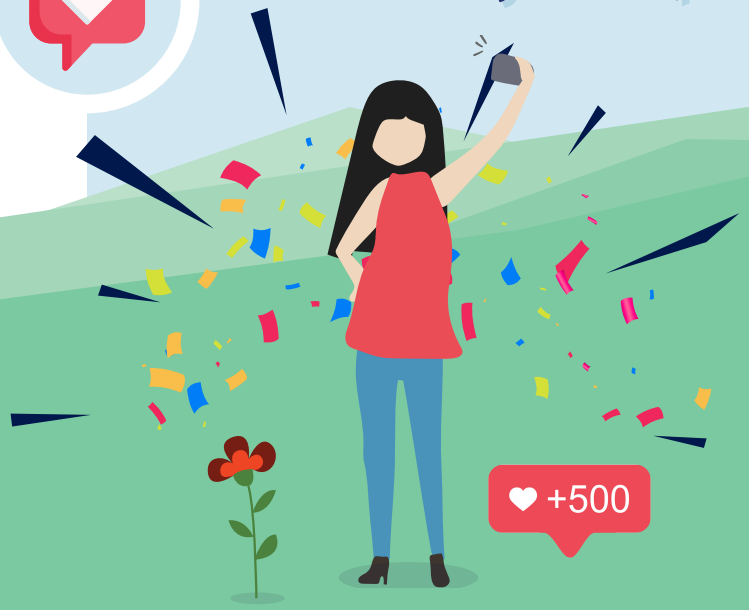
Parents

- Explain to your children what they may share, publish, download, or to what they may say «I like» on the internet
- Explain to your children that negative messages or comments create disadvantageous footprints
- Act exemplary for your children by taking care of your own online presence / profile. Spend time to joint web activities with your children
- Advise your children to inform you if they encounter anything that scares, upsets, worries or exposes them on the internet as also to keep evidence and do not respond aggressively

Teachers

- Provide examples of positive online content to the students
- Organize lessons and educational activities focusing on the impact that positive and negative footprints have for the subsequent life of the students
- Help students understand that potential negative footprints are likely to be serious obstacles to their future social, personal and professional choices
- Explain to students that excessive exposure of their lives on the internet ultimately leads to the restriction of their civil liberty

Digital Reputation



Students

- Think before you post
- Avoid inappropriate pictures
- Information can be permanent
- Lock down privacy settings on your digital devices
- Google yourself

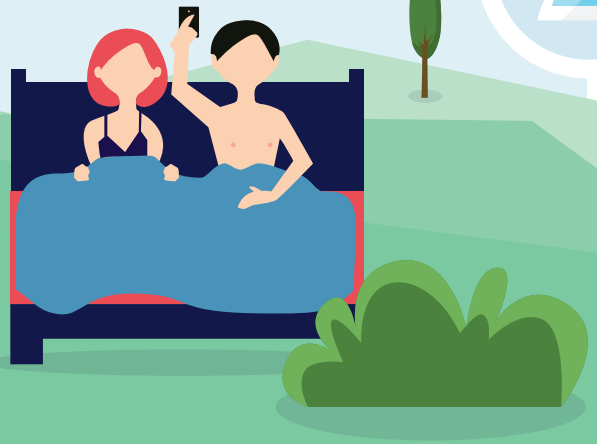
Parents

- Become role model
- Manage children's digital footprint
- Protect children's digital privacy
- Encourage discernment
- Talk regularly with your children about online issues
- Monitor children's online reputation

Teachers

- Inform your students that their Internet profile stays with them forever
- Inform your students about online privacy
- Inform your students that their online actions affect others
- Motivate your students to keep personal information private
- Advise your students to have a positive digital footprint

Sexting



Students

- Think twice before taking a naked or semi-naked photo
- Remember that photos can be distributed to many people in the future
- What will happen with your photos if you break up with your boyfriend/girlfriend?
- Are you pressured by your peers to be «fashionable»?
- If your mobile device is stolen, what will happen then to your photos?

Parents

- Be informed and discuss calmly about potential dangers of digital sharing personal photos / messages
- If critical incidents occur, inform dedicated organizations / government initiatives
- Keep an open communication channel with children about their online choices and habits
- Observe strange behaviors and changes to your children
- Discuss and support your children if they seem anxious and are ashamed to speak

Teachers

- Inform your students about sexting
- Encourage your students to speak to a trusted adult if they get any photos or messages (or requests for photos) that make them uncomfortable
- Raise awareness of the risks
- Build a culture of communication between students and principal teaching / support staff
- Show students how to report inappropriate behavior

Sextortion

Students

- Reject friend request from strangers and do not communicate online with people you do not know
- Use wisely the camera of your digital device and only with people you really know
- Never reveal yourself (i.e. naked) in front of your digital camera in a way that you may feel uncomfortable in the future
- Do not share, send or post online personal photos or videos with sensitive content
- If you have been exposed to online sexual abuse or extortion, try to stay calm, immediately stop communicating with the offender and share this incident to someone you trust

Parents

- Help your children to enable all necessary privacy settings in social media apps to safely adjust what personal info will be public available
- If your children have been exposed to online sexual abuse or extortion, try to make them feel comfortable about seeking help and protection and ask them if they prefer to talk with an expert for confidential support and consultation
- If your children have been exposed to online sexual abuse or extortion and the offender belongs to the school community, inform the head teacher and collaborate with the school staff

Teachers

- Mention to your students that they must not share and post online personal photos or videos with sensitive content
- Show your students how to enable all necessary privacy settings in their social media apps to safely adjust what personal info will be available online
- Motivate your students to use malware protection software and have installed the latest security updates of their operating system, thus reducing the chance of trojan malware to activate and control their camera
- If your students have been exposed to online sexual abuse or extortion, show them how to keep evidence (i.e., screenshots, chats, e-mails) and close collaborate with their parents

Internet Addiction

Students

- Be honest to yourself: admit it if you are in danger of internet addiction
- Set your own limits - limit internet use – especially during night hours
- Participate in activities without internet use – get a hobby – hang out with friends – go for a walk
- Accept that not all messages/emails must be answered
- Remember: Internet is just a service, people are more important
- Talk to parents/teachers/ friends – get help if needed

Parents

- Set limits - limit time and the amount of data or texts a kid can use – limit use of internet during night hours
- Communicate with your kids about Internet Addiction issues
- Spend time with your children –encourage them to spend time with friends
- Encourage your children to get a hobby (not related to internet use)
- Try to detect sudden changes of your children related with their online behavior (if they are tired/sleepy, signs of depression, etc)
- Ask for help (from professionals)

Teachers

- Set a good example
- Communicate with your students about Internet Addiction issues
- Make them aware of the dangers
- Try to detect sudden changes of your students related with their online behavior (lack of concentration, lower performance at school, etc)
- Discuss matters with parents and specialists

Identity theft

Students

- Do not forget to logout if you are using a public-shared computer
- Trust the passwords of your favorite online and social media apps and services only to your parents
- Change regularly the passwords, prioritizing sensitive accounts first
- Use different and hard to guess passwords for your social networking and internet accounts
- Immediately inform your parents if someone impersonates you with a fake social media account and report it to the social networking site to resolve the problem

Parents

- Encourage your children not to easily share online their personal data
- Encourage your children to avoid log-in to online services (i.e., e-banking) through a public network or a shared computer and provide sensitive personal or financial data. Advise them to perform these tasks through the secure private home network
- Check regularly the online digital footprint of your children to potentially eliminate or limit harmful online experiences
- If you are informed that someone is impersonating online your child, validate this and then report it to the related social networking site or to the authorities to resolve the problem

Teachers

- Remind your students to logout from a public shared computer in order to minimize the risk someone grant access to their account
- Teach your students how to wisely manage the passwords of their online accounts
- Show your students how to install and update antivirus and anti-malware software on their personal computers to boost protection from a more diverse range of online threats
- If you know the person who has stolen or misappropriated a student's online identity (i.e., creating an account with student's name), ask kindly to delete this online account
- Consider storing students' personal info for as long it is necessary and make sure that is safely deleted from the storage devices

Meeting with strangers

Students

- Think twice before you start an online chatting with an unknown person
- Photos in your «friend's» account may be fake
- Never give your personal data in a chat room
- If a conversation made you feel uncomfortable, keep a copy and make a complaint to a dedicated organization or a government initiative
- When seeking help, always go to a trusted adult

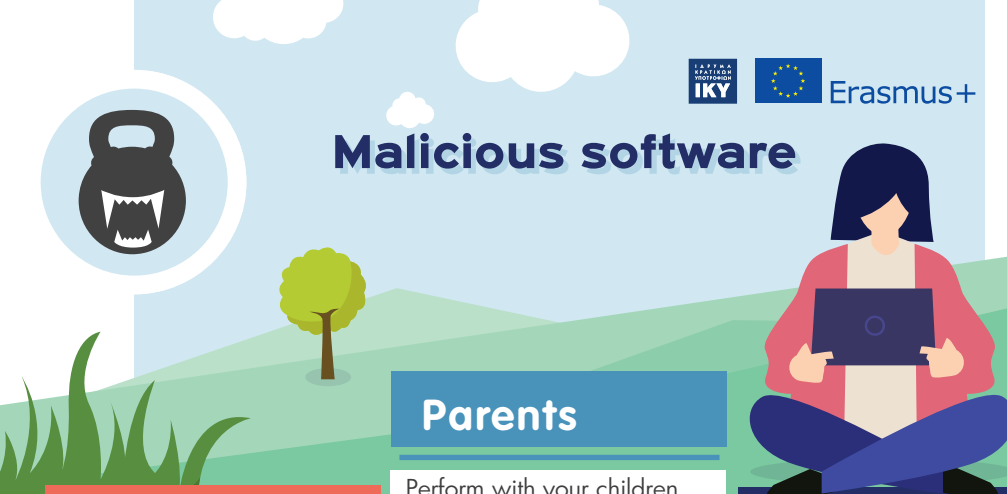
Parents

- Show your children the security options available on social networking sites
- Inform them that the person they are talking online may not be the one s/he looks like
- Keep an open communication channel with children about their online choices and habits
- Make sure you know who s/he is talking or playing online
- Ensure that you create a trustworthy environment where your children communicate every concern they may have

Teachers

- Inform your students about the topic "Meeting with Strangers"
- Alert your students for the risks when they provide personal information in a chat room
- Engage students in conversations with real incidents
- Help your students set their own limits and if an online conversation makes them feel uncomfortable or embarrassed, advise them to keep a copy

Malicious software



Students

- Be sure to install the latest operating system and security updates on your computer or digital device
- Do not install software of unreliable or unknown sources on your computer because it may contain viruses, worms or other kinds of malware
- While navigating online try to avoid dubious and non-recommended websites
- Ignore messages or pop-up windows that ask you to disable your computer's security systems
- While navigating online, if a pop-up window asks you to perform an Internet virus check, ignore it because it will potentially attempt to fraudulently steal your personal information or install malicious software

Parents

- Perform with your children regular checks on their computers with anti-malware and anti-spyware software to detect and potentially remove any infections found
- Navigate online with your children and help them to identify and understand potential risks from malicious software and advise them how to safely address various online threats
- Inform your children that peer-to-peer applications and file-sharing technologies introduce security threats that may put their computers at risk
- Advise your children not to open emails and attachments from unknown senders to avoid exposing their computers to viruses, worms, and trojans
- Inform your children that their mobile devices can be potentially affected with malicious software

Teachers

- Emphasize to your students that is high priority to install antivirus software to their computers and update it frequently
- Implement educational scenarios to inform your students about the risks of malicious software while browsing the Internet or using their e-mail as also to motivate them to efficiently address online threats
- Draw attention to your students to regularly backup their data as an essential task to protect their important files and prevent data loss
- Create various examples of strong and unique passwords with your students for their operating system and online accounts and emphasize the need to change or update them frequently

Fake news

Students

- How to identify fake news: consider the source, the author, the date, spelling errors and hyperlinks
- Cross-check with other online sources
- Carefully observe online media (i.e., photos)
- Don't share fake news
- Don't trust everything you see or read online

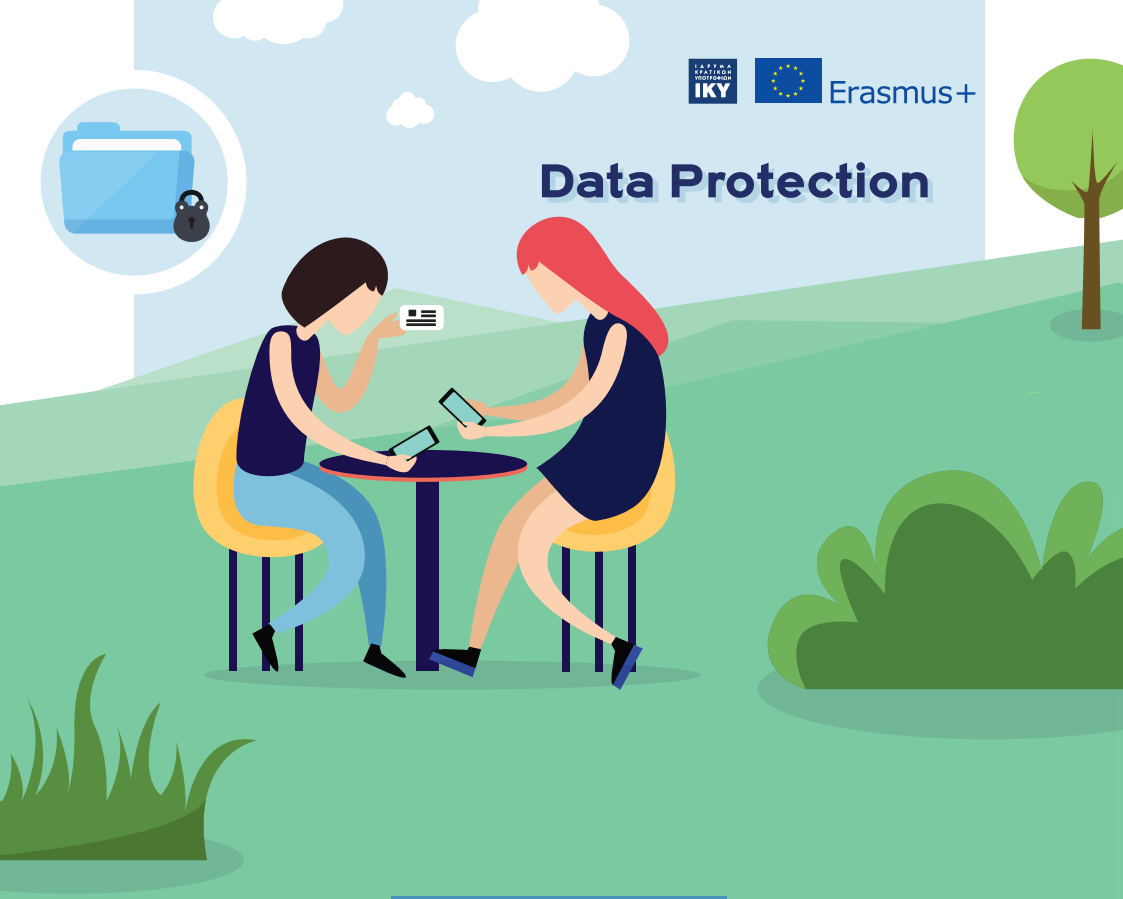
Parents

- Help your children to have critical thinking on what they see and read online
- Encourage children to develop common sense online
- Remind your children that they can always ask you to help them determine what is real
- Identify with your children the difference between mistakes and lies
- Motivate your children to get a balanced feedback by checking several sources – not just one

Teachers

- Teach Critical Thinking Skills in your classroom
- Teach your students how to distinguish Opinion from Fact
- Look for resources and lesson plans on how to address the spread of online disinformation and fake news
- Advise your students how to safely navigate and wisely evaluate online information
- Explore with your students various news or events through different online sources and make qualitative comparisons

Data Protection



Students

- Make your passwords private
- Think before you post
- Don't forget to log out
- Keep your digital device safe
- Lock down privacy settings

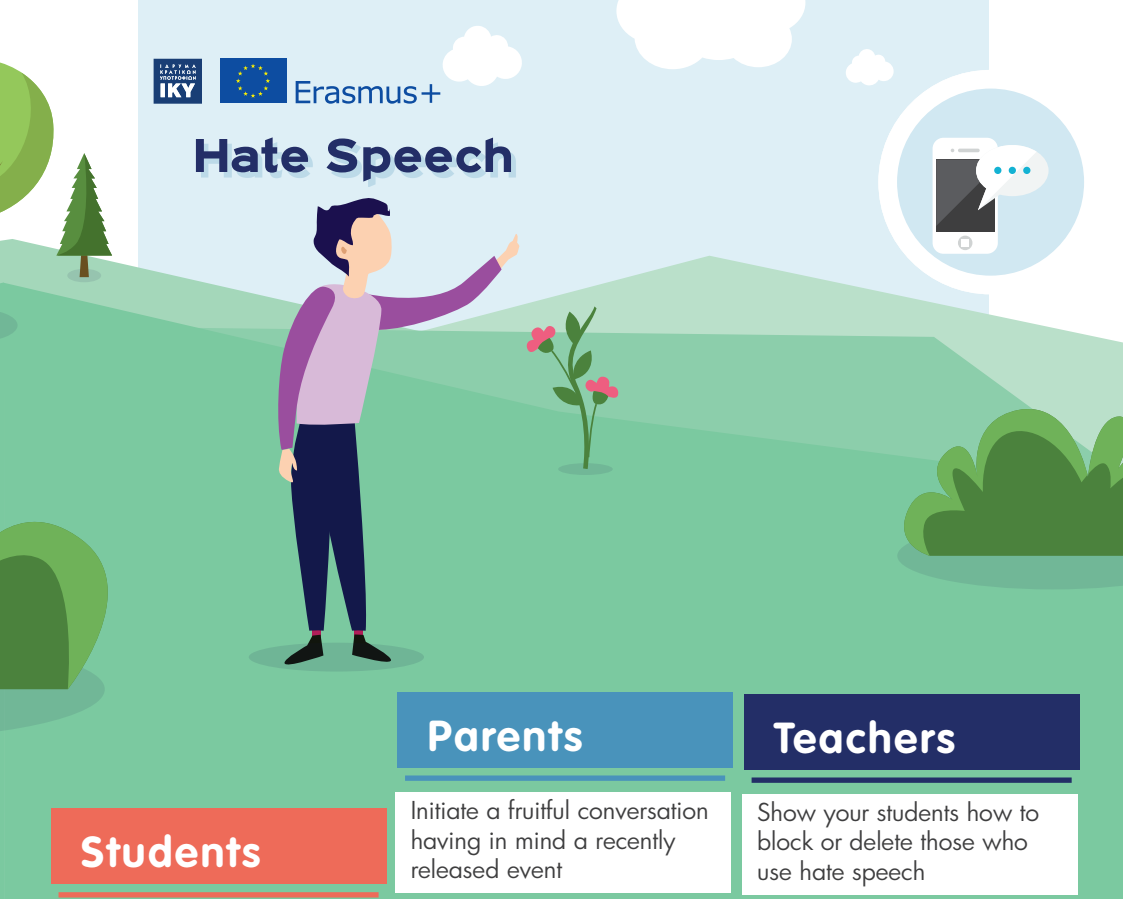
Parents

- Set limits
- Protect the data privacy of your children
- Limit the amount of data or sms your children can use on their mobile devices
- Discuss with your children about data privacy issues
- Let your children know that they can depend on you if they make a privacy mistake

Teachers

- Set a good example
- Teach your students that personal data is valuable
- Keep up with Digital Technology and data protection issues
- Make password protection priority
- Emphasize the importance of protecting mobile devices

Hate Speech



Students

- Talk with your parents or teachers and ask for their help
- Report hate speech incidents to local authorities or national bodies.
- Block or delete users who adopt threatening or abusive behavior
- Don't share posts that incite hate speech content
- React to hate speech by publishing your own positive and calm statements

Parents

- Initiate a fruitful conversation having in mind a recently released event
- Cultivate empathy to your children and help them to care those from different backgrounds
- Explain your family values and views regarding racism, xenophobia and other forms of hate speech and violence
- Keep an open communication channel with your children and build a good rapport with them
- Help your children to develop a critical approach to online content

Teachers

- Show your students how to block or delete those who use hate speech
- Inform your students about European policies and educational tools to address and combat online hate speech
- Promote reliable online content advancing the idea of no hate speech
- Prevent and counter hate speech through human rights education
- Motivate your students to organize or participate in youth actions and events against hate speech

Radicalization

Students

- Be critical on what you see or read online
- Block web-pages that promote extremist propaganda content
- Discuss online extremism issues with a person you trust
- Get support and guidance from national agencies and helplines
- If you're worried about a friend's behavior, you should consult a person you trust

Parents

- Look for guidance on how we approach children about online radicalization
- Have a fruitful conversation with your children about extremism and radicalization
- Safeguard in time your children and vulnerable people from online extremism
- Install parental control apps so that you can monitor what they access online
- Be aware on your children behavior changes and the adoption of extremist views

Teachers

- Organize school activities and events to raise awareness on radicalization
- Search for teaching tools and adopt best educational practices to combat radicalization
- Initiate fruitful discussion with your students based on recent news events
- Detect and respond to signs of potential or imminent radicalization and protect vulnerable students
- Help your students understand and reject online information provided by violent extremist groups

Misleading advertisements and scams

Students

- Have you ever wondered why many products on the internet are offered to you for free?
- Think about; how social networking services make money?
- Do you know that social networking services make targeted ads based on the personal information (i.e., age, gender, interests etc) you have entered in your profile?
- Do you know that there are fraudulent messages to extort money and personal bank account details?
- Have you ever thought that a message you get in your email account asking for your personal information is fraudulent?

Parents

- Inform yourself and discuss calmly about the potential dangers of misleading ads and SMS phising (smishing)
- If serious incidents arise, contact dedicated agencies or organizations
- Protect your children from annoying pop-up windows using software that blocks them
- Use search engines oriented for kids or search engines with parental controls
- Support your children and have a fruitful discussion if they are anxious and are ashamed to speak

Teachers

- Inform your students about misleading advertisements and scams
- Give examples of commonly seen misleading ads, and identify the deceptive techniques used in each case
- Discuss with them the risks (i.e., when revealing their passwords)
- Ask students to look for and present to class ads they find online that they think are fraudulent or misleading.
- Teach your students to reject suspicious and tempting messages

Bad behavior, comments, gossip

Students

- Ignore or block the offender from contact or communication
- Do not believe everything that is posted
- Ask for help
- Record (get proof)
- Think before you post
- Don't make, in revenge, any offensive comments

Parents

- Communicate with your kids about bad behavior – comments – gossip on the internet
- Try to detect sudden changes in your children's' online behavior (i.e., exposure to porn, etc)
- Spend time with your children
- Ask for help (from professionals)
- Improve knowledge of the internet, social media and ICT

Teachers

- Discuss with your students about bad behavior – comments – gossip on the internet
- Make them aware of the dangers
- Show them how to get help and report an inappropriate behavior / posting
- Try to detect sudden changes in your students' online behavior (i.e. avoid its use, signs of depression, lower performance at school, etc)
- Discuss matters with parents and specialists
- Improve knowledge of the internet, social media and ICT

Digital games - risks from online games

Students

- Prefer direct contact with your friends and the real game
- Do not neglect your other activities and obligations
- Protect your personal data when playing online games
- Have a critical mind and distinguish information from advertising content
- Make frequent breaks during online gaming

Parents

- Inform yourself and discuss calmly about online gaming dangers and risks
- If serious incidents arise (i.e., excessive engagement), contact dedicated organizations / agencies
- Keep game technology in shared family space
- Observe strange behaviors and changes to your children (i.e., anger, depression)
- Support your children and have a fruitful discussion if they seem stressed and isolated

Teachers

- Tell your students about the dangers of online games (i.e., credit card fraud, sexual harassment etc)
- Inform your students about pros and cons of playing online games
- Raise awareness of the risks (i.e., promotes poor health) and help students to stay safe
- Motivate students to enjoy online apps and games with minimal risk
- Learn students how to set gaming time limits and report serious behavioral issues

Online gambling

Students

- The minimum legal age for most types of online gambling is 18
- Online gambling can be very addictive and is associated with poor physical and mental health
- Online gambling is risky, and it can seriously affect your financial and social status
- Perform wisely payments related to online gambling and inform your parents about these activities
- Always remember that online payments are directly related with real money

Parents

- Talk to your children about online gambling apps and emphasize on those offered for free
- Make sure your children do not have access to your credit/debit cards and they are not linked to shared digital devices
- Use parental control apps and filtering software that blocks access to online gambling sites
- Identify early signs that your children are developing problems with online gambling
- Be a role model to your children and adopt a responsible behavior on your online gambling activities

Teachers

- Inform your students about age limitations in order to participate in various forms of online gambling
- Talk to your students about the potential harmful effects of online gambling
- Explain your students the basic online gambling processes and the odds of winning with simple math-oriented scenarios
- Advise your students about online gambling advertising in social media apps or sites
- Remind to your students that online gambling apps or sites may be vulnerable to privacy violation

Managing access to dangerous content

Students

- You can report a web-page promoting illegal actions
- Online videos that incite others to act violently, are strictly prohibited
- You can report a website illegally displaying cigarettes, alcohol and on-line gambling
- Your online behavior potentially affects you offline
- You may contact a dedicated organization or a government agency, if you feel uncomfortable or threatened, during your online browsing

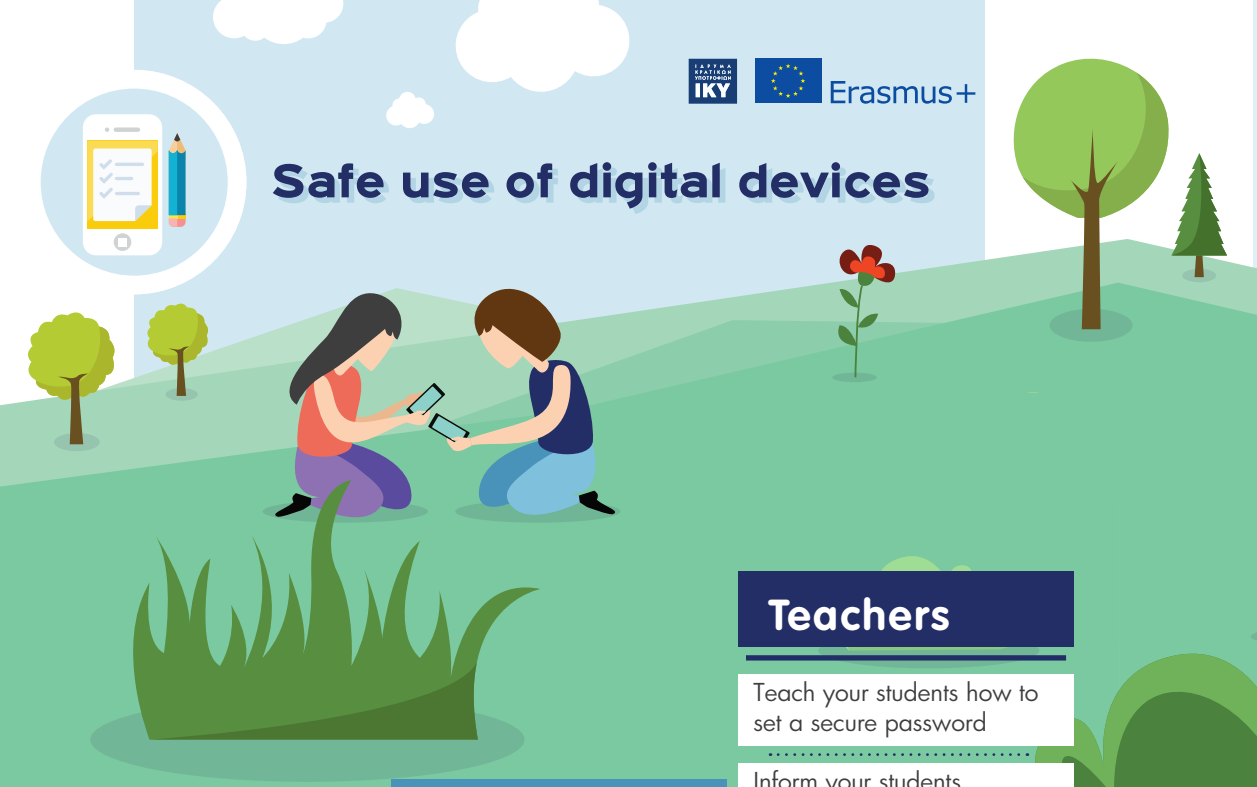
Parents

- Establish a home-based «Acceptable Use Agreement» for proper internet browsing
- If serious incidents occur, contact dedicated agencies or organizations
- The most important safety measure against dangerous online content is communicating with your children
- Create possible scenarios addressing and reporting dangerous online content
- Encourage and discuss with your children if they seem stressed and afraid to talk about high-risk Web content

Teachers

- Inform your students about high-risk web content (i.e., pornography, online gambling etc)
- Alert your students about the dangers of accessing high-risk web content
- Initiate fruitful conversations with your students focusing on real cases and best practices or guidelines
- Advise students on how to report harmful or inappropriate web-content
- Take an active role in your students' Internet activities and ensure that they benefit from them without being exposed to harmful content

Safe use of digital devices



Students

- Protect your digital device with a strong password
- Stay in-line with family's rules and screen time limits
- Don't give out your mobile number and don't reply to unknown text messages
- Remember to disable Wi-Fi and Bluetooth when not in use
- Don't access private information using public Wi-Fi networks

Parents

- Apply family rules and set screen time limits
- Keeping your software up to date is the best defense against online threats
- Show your children how to take advantage of the "Lost and Found" functionalities of their smart devices
- Try not to retain sensitive data longer than necessary to your mobile devices
- Make sure to safely remove any sensitive data when you dispose of a mobile device

Teachers

- Teach your students how to set a secure password
- Inform your students about "Location Services", Bluetooth, Wi-Fi and GPS and why they should be disabled when we don't need them
- Tell your students about malicious software and advise them to use anti-virus and anti-malware software to protect their digital devices
- Remind your students that timely installation of software updates is important to protect and secure both their privacy and personal data
- Advise your students on how to respond to mobile phone bullying and deception.

Safe use of Social Media

Students

- Think twice before hitting "Enter"
- Use privacy settings
- Be cautious of Friend requests
- Be nice and polite
- Never meet strangers offline

Parents

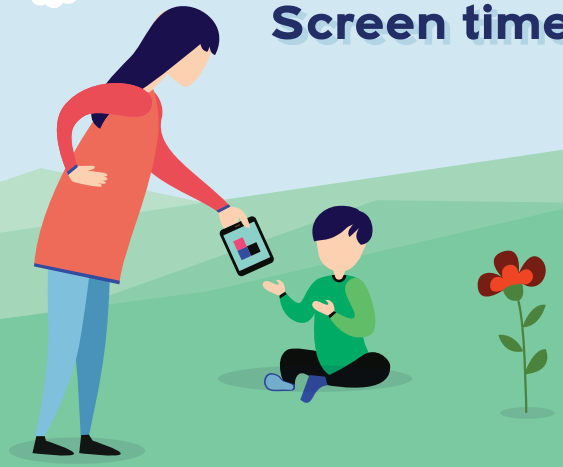
- Self-educate about social media
- Talk to your children about the dangers and the consequences of social media
- Set rules and limits
- Discourage your children from posting their location, home address and phone number
- Set a solid relation of trust and communication

Teachers

- Set a good example
- Talk to students about pros and cons of social media use
- Raise awareness of the risks
- Engage students in real conversations
- Learn students how to report inappropriate behaviour

Erasmus+

Screen time



Students

- Take care not to miss your walk or your game in the neighborhood or the playground just to spend a little more time with your favorite digital device
- Include some sports or outdoor activities in your daily program
- When you need help, you can consult an older person you can trust (i.e., siblings, parents, teachers)
- Prefer to have your meals in the dining-room rather than in front of the TV or your laptop
- Take care not to spend too much time in front of the PC or the laptop

Parents

- Formulate a weekly schedule together with your children, to properly manage their screen time
- Be a positive role model and set examples for prudent use of digital devices
- Play digital games with your children, following reasonable time limits
- Place PC and other digital entertainment technologies in shared family areas
- Remember, that bedroom is a place to rest, relax and restore energy

Teachers

- Inform your students about the dangers of excessive screen time and raise awareness for related physical and mental health issues
- Collaborate with your students to develop and promote off-line activities
- Help your students to enjoy off-line entertainment and social activities
- Advise students to enable and access the screen-time daily or weekly reports on their mobile devices
- Motivate your students to make unplugged playtime a daily priority

Authors

Dr. Chlapanis Georgios- Errikos, 2nd Upper Secondary School Kos
Karagiorgou Eleftheria, 7th Upper Secondary School Trikala
Katsaros Athanasios, 2nd Lower Secondary School Galatsi
Papanastasiou Georgios, 6th Primary School Agia Paraskevi
Tryfonidoy Styliani, Lower & Upper Secondary School Tychero, Evros
Dr. Zarouchas Thomas, Computer Technology Institute & Press "Diophantus"

eSafety Label National Coordinator

Louvris Aris, Regional Directorate of Primary and Secondary Education of Western Greece

Graphic Design

Stasinou Stavroula, Computer Technology Institute & Press "Diophantus"

Contact

Louvris Aris, louvris@sch.gr
Dr. Zarouchas Thomas, zarouchas@cti.gr

Tips&Advice

SECURITY POLICIES for SAFER INTERNET

Tips for Students, Parents and Teachers

eSafety Label
for a safer school

Safer Internet Centres (SICs) across Europe
For more information about safe internet use, get in contact with
the national experts using the helpline of your country by following the link below:
https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope

ΙΔΡΥΜΑ ΚΡΑΤΙΚΩΝ ΥΠΟΤΡΟΦΙΩΝ
ΙΚΥ
Erasmus+
2017-1-EL01-KA201-036242