

A large network diagram of diverse people icons connected by dashed lines, with two large blue circles containing the title text.

GUIDE FOR TEACHERS AND PARENTS

INTERNET SAFETY

Guide - *noun* - one that leads or directs another's way / something that provides a person with guiding information

Guide - *verb* - to act as a guide to : direct in a way or course / to superintend the training or instruction of



Title: *Internet safety – Guide for teachers and parents*

Manuscript completed in october 2022

Erasmus + - Project no: 2020-1-PL01-KA229-081405- “CLICK SAFE, SURF SMART, BE AWARE OF WHAT YOU SHARE.”

COPYRIGHT NOTICE

“Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by-nc-sa/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated”.



Attribution- NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

You are free to:

Share — copy and redistribute the material in any medium or format

Adapt — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for commercial purposes.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.



Contents

The Convention on the Rights of the Child	3
Human Rights for Internet Users	5
Creating safe spaces for kids - parents	6
Internet safety - Teachers	16
References	24



The Convention on the Rights of the Child

We start this guide referring some rights written in The Convention on the Rights of the Child (The children’s version):

Number 15. Setting up or joining groups

Children can join or set up groups or organizations, and they can meet with others, as long as this does not harm other people.

Number 16. Protection of privacy

Every child has the right to privacy. The law must protect children’s privacy, family, home, communications and reputation (or good name) from any attack.

Number 17. Access to information

Children have the right to get information from the Internet, radio, television, newspapers, books and other sources. Adults should make sure the information they are getting is not harmful. Governments should encourage the media to share information from lots of different sources, in languages that all children can understand.

Number 19. Protection from violence



“CLICK SAFE, SURF SMART, BE AWARE OF WHAT YOU SHARE.”

Governments must protect children from violence, abuse and being neglected by anyone who looks after them.

Number 29. Aims of education

Children’s education should help them fully develop their personalities, talents and abilities. It should teach them to understand their own rights, and to respect other people’s rights, cultures and differences. It should help them to live peacefully and protect the environment.



Human Rights for Internet Users

On the other hand, in the **Guide to Human Rights for Internet Users** adopted on 16 April 2014, the Committee of Ministers of the Council of Europe laid down the basic framework of principles to protect the fundamental human rights guaranteed by the **European Convention on Human Rights** for all internet users.

The guide emphasizes that the protection of the right to freedom of expression, access to information, the right to freedom of assembly, protection from cybercrime, the right to a private life, and the protection of personal data are all equally protected online and offline [Guide to Human Rights for Internet Users, Council of Europe].

YOUR DIGITAL RIGHTS IN BRIEF

Access and non-discrimination

Freedom of expression and information

Freedom of assembly, association and participation

Privacy and data protection

Education and literacy

Protection of children and young people

Right to effective remedies for violations of human rights



Creating safe spaces for kids - parents

Around one in three internet users is a child, and these children are getting into the Internet at ever-younger ages through various devices. They are spending more and more of their time on the Internet, browsing social media, playing online games and using mobile apps.

This frequently happens without adult supervision.

While the Internet offers many occasions for learning, communication, creativity and entertainment, it also opens up certain dangers to susceptible users such as children.

For families around the world, the fundamental responsibility of **parents** and the aims of parenting remain unaffected: parents are still obliged to nurture, to protect, to provide for, to love, to connect with and to guide their children as written in The Convention on the Rights of the Child previously referred.

Parents are responsible for the physical care of their children, and for their education leading them to a status as productive adults.

These models and values need to reach out the online world in order to connect traditional values and the online world.



Digital parents must understand and use privacy settings on social media accounts and be aware of their child’s digital footprint and identity.

Parents must also **establish appropriate limits to their child’s online activities preferably in line with suggestions of the national authorities**. Parents should also watch their own behaviors as parenting in the digital age, for example, how they share online images and their own use of digital technologies.

Parents are commonly the first ones to provide technology to their young children, and therefore they need to dominate a reliable understanding of what young children may come across in the digital world.

<https://pixabay.com/pt/vectors/mulher-computador-port%C3%A1til-caderno-1459220/>



What to do as a parent?

Positive digital parenting **respects children’s rights online** and use conversations and trust. They also offer kids real-life alternatives to digital activities. Nevertheless, five essential tools must take place in families: **communication, critical thinking, citizenship,**

continuity and community [in PARENTING IN THE DIGITAL AGE, Dr Elizabeth Milovidov, JD].

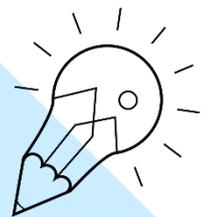




What to do?



<https://pixabay.com/pt/vectors/mulher-computador-porf%3a1fil-caderno-1459220/>



Communication:

Parents should talk with their child and ask them:

1. “Who are you talking to online (classmates, friends in town/abroad, strangers)?”
2. “What are you doing online?”
3. “Where are you going online (type of websites, platforms, etc.)?”
4. “When are you going online (for how long and at what time of the day)?”

These questions can extend into an in-depth conversation with children or adolescents.



What to do?



<https://pixabay.com/pt/vectors/mulher-computador-port%C3%A1til-caderno-1459220/>



Critical thinking:

1. One should reflect upon what to do, before acting.
2. Parents must reflect and decide if family really needs some new device, game, app, robot or technology. After acquiring they should think of conducts to use it safely and responsibly, (maximizing privacy and data protection settings, and defining when and for how long digital technologies may be used). Technology, and the internet also have risks to people's health, safety, autonomy, or privacy. Thinking critically is important to ensure a safe and healthy online development for children.



What to do?



<https://pixabay.com/pt/vectors/mulher-computador-port%C3%A0til-caderno-1459220/>



Citizenship

As parents and caregivers, you can support digital citizenship education for your children: by getting involved in an internet and citizenship dialogue; by helping your children balance the social and interpersonal implication of using online technology (within certain limits); and by communicating regularly with them and their educators, in order to help develop their skills as involved and informed digital citizens, appropriate to their respective ages.



What to do?



<https://pixabay.com/pt/vectors/mulher-computador-port%C3%A1til-caderno-1459220/>



Continuity

Once parents have begun to have those conversations with children, it is necessary to continue the communication, even when the subject matter is uncomfortable.



What to do?



<https://pixabay.com/pt/vectors/mulher-computador-porf%3a1fil-caderno-1459220/>



Community

Sometimes in daily family life, we should turn to a family member or to a community member solve an question.



Golden guidelines:

Teach your kids **appropriate online behavior**.

Keep the computer in a common area where you can **watch and monitor** its use, not in individual bedrooms.

Monitor time spent on smartphones or tablets. Set time limit according to age.

Bookmark kids' favorite sites for easy access.

Check your **credit card and phone bills** for unfamiliar account charges.

Find out what, if any, **online protection is offered** by your child's school, after-school center, friends' homes, or any place where kids could use a computer without your supervision.

Take your child **seriously if he or she reports an uncomfortable online** exchange.

Turn off devices during meals and at least 1 hour before bedtime.

**And remember...always remember that
you should be a good example!**



Always advise your children to:



Follow the family rules.

Never **post or trade personal pictures**.

Never **reveal personal information**, such as address,
phone number, or school name or location.

Never give out the **real name** and **don't share passwords**
(other than with parents).

Never agree to **get together in person with anyone met
online** without parent approval and/or supervision.

Never **respond to a threatening email**, message, post, or
text.

Always tell a parent or other trusted adult about
any **communication or conversation**
that was scary or hurtful.



Warning Signs



<https://pixabay.com/pt/illustrations/seguran%C3%A7a-seguro-prote%C3%A7%C3%A3o-osh-1004644/>

- Spending long hours online, especially at night.
- Phone calls from people you don't know.
- Unsolicited gifts arriving in the mail.
- Your child suddenly turning off the computer or other device when you walk into the room.
- Withdrawal from family life and reluctance to discuss online activities.



Internet safety - teachers

Teachers must have know-how of online rules to ensure security, regardless of his/her subject area.

As technology continues to be such a huge part of students' lives, from communicating with others to searching content they enjoy, it has a real influence on school life.

While online learning provides so many positive opportunities for learners and teachers alike, it is more important than ever to reinforce cybersecurity defenses to deal with new and emerging attacks.

The European Union Agency for Cybersecurity (ENISA) *continues to raise citizens' awareness to cybersecurity and potential cyber threats (e.g. phishing attacks, botnets, financial & banking frauds, data fraud), providing guidance on [good practices](#) to promote safer online behavior (e.g. cyber-hygiene and cyber-literacy). Furthermore, aligning its actions with the EU's Digital Education Action Plan¹, ENISA is promoting and analysing cybersecurity education, in order to tackle the cybersecurity professional shortfall, which represents an issue for both economic development and national security (<https://www.enisa.europa.eu/>).*

To know additional information on raising awareness of cybersecurity [read ENISA report here](#) and find out, for example, how some countries manage safety campaigns (pages 37 to 51).

¹ The Digital Education Action Plan (2021-2027) is a renewed European Union (EU) policy initiative to support the sustainable and effective adaptation of the education and training systems of EU Member States to the digital age.



“CLICK SAFE, SURF SMART, BE AWARE OF WHAT YOU SHARE.”

Remember that there should be no lasting or permanently accessible record of the content created by children on the Internet if it poses challenges to their dignity, security and privacy or renders them vulnerable now or at a later stage in their lives².

² Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, adopted on 20 February 2008



Advices for teacher working in the school



Use **apps and platforms authorized by the Department of Education or school**. If you want to use one which wasn't reviewed by it, you should ask for a review and if authorized, and then use it.

The **school hardware** should be used exclusively for **professional purposes**.

Warn the tech responsible if anything is wrong with the system or if you notice any irregularities.

You should **scan for virus**, pen drives or similar before you use it.

Every file received from emails or similar should be scanned by the antivirus before the download.

Keep the hardware and software **clean after the usage**.

Use the **appropriate user** when signing into the computer.

Always **sign out** of your session when leaving the computer.

Don't login to bank accounts in the workspace.



“CLICK SAFE, SURF SMART, BE AWARE OF WHAT YOU SHARE.”

Don't login to our **social network** accounts in the workspace.

Avoid **opening links/files** from unknown sources.

Always **clear the browser history** when leaving the computer.

Use **strong passwords** for educational apps and platforms.

Avoid **saving your login credentials** unless using your own computer.

Avoid **writing passwords** in front of anyone.

Be **aware of what your students are doing** on their computers, both hardware and software could be damaged without you knowing.

Avoid using pen drives or similar hardware, **use google drive or similar** platforms instead.

Verify the **security of the websites, apps or extensions** before using them.



Creating safe spaces for students in the classroom

Teach students about copyright:

When upload, copy information or link content in your online classroom advise them to pay **attention to copyright** and only post what you have rights to use.

When visiting sites during class:

Check sites before showing in class or suggesting to students.

Teach students about Phishing:

Phishing is the practice of tricking users into **giving out private information**, such as usernames and passwords. This can lead to identity theft or other privacy violations.

Give students some basic tips for avoiding phishing schemes:

Don't **open emails** or messages from people you don't know.



“CLICK SAFE, SURF SMART, BE AWARE OF WHAT YOU SHARE.”

Don't reset accounts and passwords from links within an email.

Go directly to the official site, log in, and change your information there.

Don't open attachments (videos or files) in emails from people you don't know. These attachments often contain malware that installs on your device.

Don't share your personal information online.

Beware of offers that seem **too good to be true.**

Teach your students safety skills:

Don't connect with strangers online (including social media friend requests).

Create **secure passwords** and keep them private.

Don't share personal information that can lead someone to your location or allow them to guess your passwords (date of birth, address, school, online surveys, etc.).

If it doesn't feel right, it probably isn't. Trust your gut and tell an adult.



Teach students about safe internet search strategies

Teach your students **safe internet search strategies**. One key tip is to scan the description before clicking the link to make sure that it is really the content they want. “Look before you click.”

TIP #1

You can perform more specific searches by using **specialist search engines**. *Google Scholar*, for example, allows you to search for academic articles that might be hard to find in a general search.

TIP #2

Use **Specific Keywords** in search engines. **Remove unnecessary stop words** like prepositions (in, of, on), conjunctions (and, but) and articles (a, the) and avoid suffixes such as -ing, -s or -ed.

TIP #3



Use **Quotation Marks** in words to search for that specific word or phrase.

TIP #4

Remove Unhelpful Words (by inserting a hyphen/small dash/minus sign immediately before a word excludes it from a search).

TIP #5

Refine Your Search Using Operators - operators allow you to narrow down your internet search in a more directed way.

Wildcard Searches: use the * symbol as a placeholder for another word. For example, searching for * *man in the world* returns results for the *richest man in the world*, the *tallest*, the *oldest*, and so on.

Combination Searches: the **OR** operator enables you to search for two or more terms simultaneously. Typing *selling OR retailing*, for example, will return pages where either of the terms is used, without both needing to be present.

Another way to combine searches is to **use AND**. This operator ensures that you receive only search results that include two or more terms.

Search a Specific Site: when you type **site:** followed by the URL of the website that you wish to search and a search term, you limit your search to a single website.

Finding Related Sites: another useful operator is **related:** Typing this before of a web address that don't exactly know, your search results will deliver a range of websites that are like the website you think it is.



References

Publications:

Council of Europe for and with children, parenting in the digital age, Positive parenting strategies for different scenarios, August 2020

European Union Agency for Cybersecurity (ENISA), e-Governance Academy (EGA), RAISING AWARENESS OF CYBERSECURITY A Key Element of National Cybersecurity Strategies, NOVEMBER 2021 (<file:///C:/Users/vanda/Downloads/ENISA%20Report%20-%20Raising%20awareness%20of%20cybersecurity%20as%20a%20key%20element%20of%20NCSS.pdf>)

Janice Richardson, Dr. Elizabeth Milovidov, J.D., Martin Schmalzried, INTERNET LITERACY HANDBOOK, Building a Europe for and with children, Council of Europe, October 2017 (<https://edoc.coe.int/en/internet/7515-internet-literacy-handbook.html>)

GUIDE to hUman rIGhts for IntErnEt UsErs, Recommendation CM/Rec(2014)6 and explanatory memorandum, (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies) (<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31>)

Websites:

<https://creativecommons.org/>

<https://www.merriam-webster.com/dictionary/guide>

<https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/>

<https://parentzone.org.uk/>

https://link.springer.com/chapter/10.1007/978-3-030-87698-2_4

<https://www.unicef.org/child-rights-convention/convention-text-childrens-version>

<https://www.enisa.europa.eu/>

<https://digital-strategy.ec.europa.eu/en/policies/better-internet-kids>

<https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids>

<https://staysafe.org/>

<https://rm.coe.int/168008c37f>



<https://kidshealth.org/en/>

<https://avidopenaccess.org/resource/internet-safety-for-teachers/#1596816118905-f7807f65-59da>

Images:

<https://pixabay.com/pt/illustrations/%c3%adcone-luz-id%c3%a9ia-l%c3%a2mpada-el%c3%a9trica-4017417/>

<https://pixabay.com/pt/photos/filho-garota-jovem-caucasiano-1073638/>

<https://pixabay.com/pt/illustrations/meios-de-comunica%c3%a7%c3%a3o-sociais-conex%c3%a3o-3758364/>

<https://pixabay.com/pt/vectors/mulher-computador-port%c3%a1til-caderno-1459220/>

<https://pixabay.com/pt/vectors/aula-computador-aluna-professora-2029206>

<https://pixabay.com/pt/vectors/homem-adulto-homem-de-negocios-1459246/>

<https://pixabay.com/pt/illustrations/ficar-em-casa-coronav%c3%adrus-isolamento-5205390/>

<https://pixabay.com/pt/illustrations/seguran%c3%a7a-seguro-prote%c3%a7%c3%a3o-osh-1004644/>