School Gardens for Future Citizens

eSchool Garden

SAFETY IN DIGITAL ENVIRONMENTS

EDUCATIONAL TOOLS

ERASMUS+ 2018-1-ES01 KA201-050599

CONTENT

SAFETY IN DIGITAL ENVIRONMENTS

BY LAURA GRINDEI

laura.grindei@ethm.utcluj.ro

INTRODUCTION

At European level, the EU data protection rules (GDPR) have been reformed recently . In addition, online safety and cyber security are clearly indicated among the specific objectives of the Digital Education Action Plan (European Commission, 2018).

European Digital Competence Framework for Citizens (DigComp) is divided into five areas: information and data literacy; communication and collaboration; digital content creation; safety; and problem solving.

In DigComp, the **competence areas 1, 2 and 3** deal with competences that can be retraced in terms of specific activities and uses.

Competence areas 4 and 5 are "transversal" as they apply to any type of activity carried out through digital means. Problem solving elements, in particular, are present in all competence areas, but a specific area was defined to highlight the importance of this aspect for the appropriation of technology and digital practices.

1. INFORMATION AND DATA LITERACY
2. COMMUNICATION AND COLLABORATION
3. DIGITAL CONTENT CREATION
4. SAFETY
5. PROBLEM SOLVING

Safety includes competences on protecting devices, protecting personal data and privacy, protecting health and well-being and protecting the environment.

SAFETY ITEMS

Safety includes four items in education:

PROTECTING DEVICES:

Goals:

- ❑ To **protect devices and digital content**, and to **understand risks and threats** in digital environments.
- ❑ To **know about safety and security measures** and to have due **regard to reliability and privacy.**

PROTECTING PERSONAL DATA & PRIVACY

Goals:

- ❑ To **understand how to use and share personally identifiable information** while being able **to protect oneself and others from damages**.
- ❑ To **understand that digital services use a "Privacy policy"** to inform how personal data is used.

PROTECTING HEALTH AND WELL-BEING

Goals:

- ❑ To **be able to avoid health-risks and threats to physical and psychological well-being** while using digital technologies.
- ❑ To be able to **protect oneself and others from possible dangers in digital environments** (e.g. **cyber bullying**).
- ❑ To **be aware of digital technologies for social well-being** and **social inclusion**.

PROTECTING THE ENVIRONMENT

Goals:

- ❑ To **be aware of the environmental impact of digital technologies** and their use.

SAFETY AND SCHOOL RESPONSA-BILITY

Cybersafety is not the sole responsibility of the ICT teacher. Schools and their teachers have a responsibility to educate children and young people and address the underlying values (ethics) and responsible behaviours expected of them regardless of their physical location.

The Digital Agenda for Europe aims to have every European digital. Children have particular needs and vulnerabilities on the internet; however, the internet also provides a place of opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employa-bility.

The 'Strategy for a Better Internet for Children' proposes a series of actions to be undertaken by the Commission, Member States and by the whole industry value chain.

PROTECTING DEVICES AND DIGITAL CONTENTS

Most of the infections, attacks, security breaches etc. are usually only possible because of the connection between the digital device and the internet. Teachers must be aware that devices and digital content can be protected through several methods:

- *updating frequently the operating system of computers & devices used in schools , using strong passwords, safeguards, encryption procedures and data security, digital envelopes, encrypted signal streams, digital watermarks, authentication devices, digital signatures and copyright management tools.*

Teachers should also know the ethical and legal issues in sharing information: the misuse of data, the protection of one's own and others' data.

Which types of work are subject to copyright?

- Audiovisual works, such as TV shows, movies, and online videos
- Sound recordings and musical compositions
- Written works, such as lectures, articles, books, and musical compositions
- Visual works, such as paintings, posters, and advertisements
- Video games and computer software
- Dramatic works, such as plays and musicals

Which types of work are not subject to copyright?

- Ideas, facts, processes ,names and titles.

According to copyright law, in order to be eligible for copyright protection, a work must be creative and it must be fixed in a tangible medium. If a copyright-protected work is posted on YouTube without permission, users can use a webform to take down the video. For most copyright owners, this is the fastest and easiest way to request a copyright takedown.This form is open to any YouTube user, but should only be sent in by the copyright owner or an agent authorized to act on the owner's behalf.

The Content Verification Program is for copyright owners who have a frequent need to remove content from YouTube, and have consistently submitted many complete and valid takedown requests. Content ID is a system that helps copyright owners easily manage their intellectual property on YouTube. Videos uploaded to YouTube are scanned against a database of files that have been submitted by copyright owners. If Content ID finds material that matches one of your works, you can choose to block a whole video from being viewed, monetize the video by running ads against it, in some cases sharing revenue with the uploader, or track the video's viewership statistics..

What is Creative Commons?

CC: Creative Commons enable educators to reuse, remix and adapt resources because the copyright owner has already given permission to everyone.

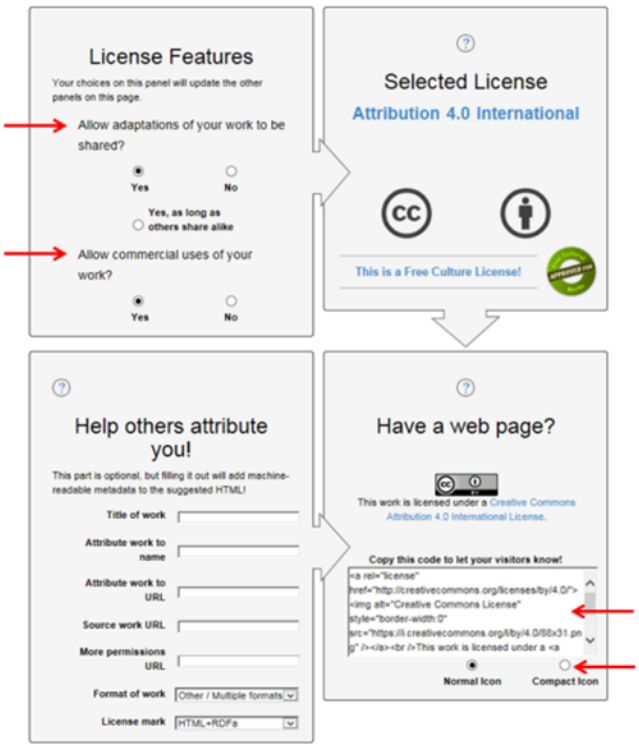
The Creative Commons Attribution license makes it easier for teachers by:

- removing complex copyright issues and concerns;
- enabling educators to reuse, remix and adapt resources without concern;
- making it free to copy and share materials for any reason; and
- removing the barriers of only being allowed to use a certain percentage of a resource and having to keep it behind a password protected system.

Applying a Creative Commons License: two ways to add the CC license:

- Simply copying and pasting the logo:
  - The normal icon or the compact icon
  - Link the icon to the license deed: http://creativecommons.org/licenses/by/4.0/

- Inserting the HTML code
  - The HTML code available: http://creativecommons.org/choose/
  - You must select 'Yes' to the two questions, and then the HTML will be produced. Note you can select the HTML for either the compact or normal icon.



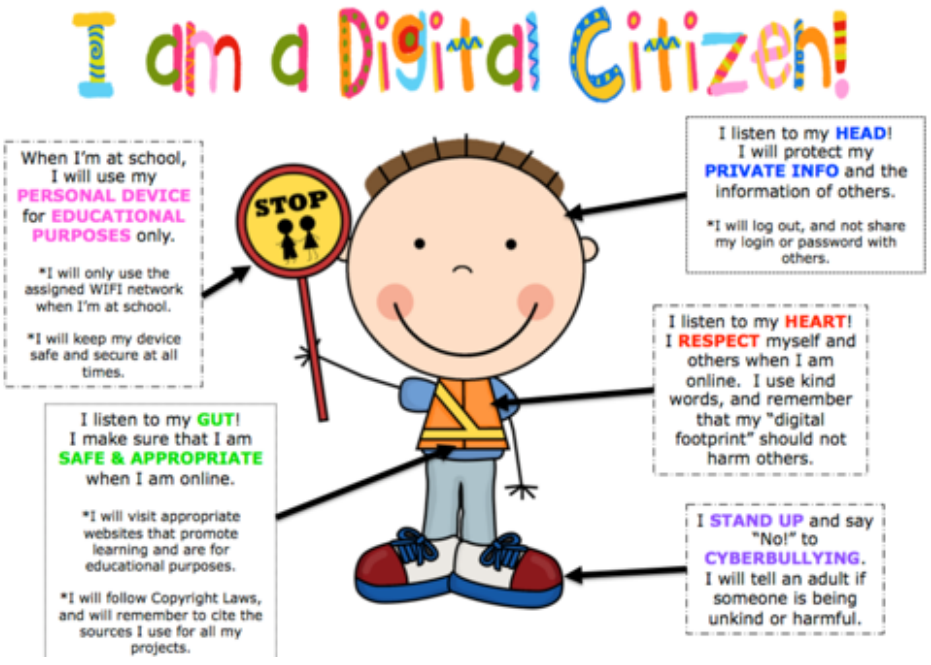
PROTECTING PERSONAL DATA & PRIVACY

This competence requires learners to protect personal data and privacy in digital environments, understand how to use and share personally identifiable information while being able to protect themselves and others from damage and understand that digital services have a 'privacy policy' to inform users how personal data is used.

PROTECT YOUR DATA - WEB BROWSERS

In the case of Web Browsers, the risk of exposure to threats is higher. We use browsers to explore the web and to use a many resources online. Each of these has its vulnerabilities.

Kids should be taught how to behave in digital world . It is important for them to understand the importance of abiding by copyright laws via the internet. Copyright images, videos, text belong to certain individuals therefore we need to obtain permission from them to be able to use, share or manipulate them.



https://www.dallastown.net

DIGITAL RISKS AND THREATS

Today there is a wide variety of risks and threats in digital environments. New threats are constantly emerging that we have to face. Here is a list of the best known today:

· ***Malware***:

- ***Viruses***: *malicious executable code that is attached to other executable files and normally replaces them. It requires to run the program to infect the device.*
- ***Worms***: *replicate themselves without human intervention by exploiting vulnerabilities. They do not alter programs, but are slowing down the network and the connected devices.*
- ***Trojan horses***: *carry out malicious action disguised as legitimate software to give an attacker remote access to the computer.*
- ***Ransomware***: *program that blocks the access to a computer until a ransom is paid. It usually propagates as a worm or Trojan .*
- ***Rootkits***: *Software that modify the operating system to create a backdoor to allow access with admin privileges to the device .*
- ***Bot***: *software that automatically perform repetitive actions and it can be used to execute malicious actions.*

· ***Email threats:***

- ***Spam***: *unsolicited messages over the internet sent for advertising, phishing, etc.*
- ***Phishing***: *fraudulent email disguised as being legitimate*

· ***Browser threats:***

· ***Spyware***: *spy on the user.*

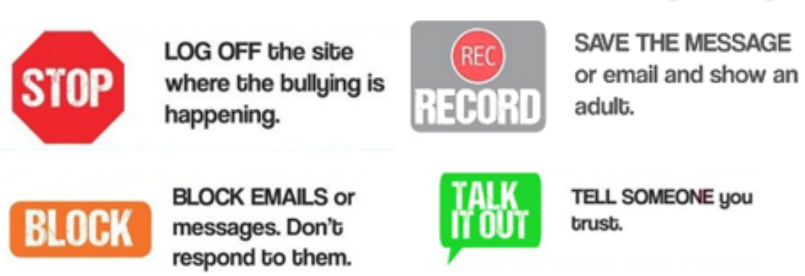
PROTECTING HEALTH AND WELL-BEING

PROTECT CHILDREN IN DIGITAL ENVIRONMENTS

The internet can be a dangerous neighborhood for everyone, but children and teens are especially vulnerable. Protecting children on the internet is a matter of awareness—knowing what dangers lurk and how to safeguard against them. Although cyber security software can help protect against some threats, the most important safety measure is open communication with the children.

CYBER BULLYING

What kids can do to stop cyberbulling?



What teachers can do to prevent cyberbulling?

- Explain students that all forms of bullying are unacceptable, and that cyberbullying behaviors are subject to discipline.
- Ask kids to report an adult if they are cyberbullying victims.
- Incorporate lessons on cyberbullying into your existing curriculum
- Ask parents to monitorize kids on line activity

WHAT MEANS CYBERSAFETY?

Cybersafety: safe practices when using the Internet to prevent personal attacks or criminal activity. Teachers could warn the children regarding the following behaviours :

- posting or participating in **bullying** (cyberbullying)
- **accessing inappropriate content**
- unwanted **contact with strangers**
- **posting or sharing personal information and passwords**
- **using (or stealing) content owned by others**, for example images, music or videos
- **plagiarising**: taking ideas or information created/ owned by others without referencing their origin
- using **critical thinking skills** when using the internet
- **accessing offensive or illegal content**
- **seeking support from a trusted adult** when there is an issue.

It is recommended that schools take a holistic approach to cybersafety education. Cybersafety practices and issues should be included within the school's curriculum planning and taught explicitly.

PLAGIARISM

Plagiarism is a highly intolerable act in the digital community, a practice that all reputable individuals are trying to avoid.

Approaches to avoid students' plagiarism:

- Teachers should review what plagiarism is and isn't, teach your students about paraphrasing and how to cite sources.
- Ensure students have plenty of time to complete their homeworks. Students tend to plagiarize or cheat when they let an assignment go to the last minute.
- Create several versions of tests and essay prompts, and alternate them year to year.
- Consider software like Turnitin, PlagScan or DupliChecker, to detect similarities to content elsewhere online, and tell students that you use them.

In theory, plagiarism is a fairly simple concept: it involves stealing the words and/or ideas of another without attribution or acknowledgment. In practice, however, there are a number of distinct aspects that constitute an act of plagiarism. Plagiarism is a highly intolerable act in the digital community, a practice that all reputable individuals are trying to avoid.

Modern technology and the development of Internet have given us access to tons of information any time we desire it and from any place on the planet. Original ideas tend to become rarer and rarer. Everybody seems to be reproducing other people's ideas and presenting them as their own. Although this practice is not anything new, a lot of people might argue that nowadays it has reached its peak.

turnitin

Plagiarism Detector

Check Plagiarism

Dupli Checker

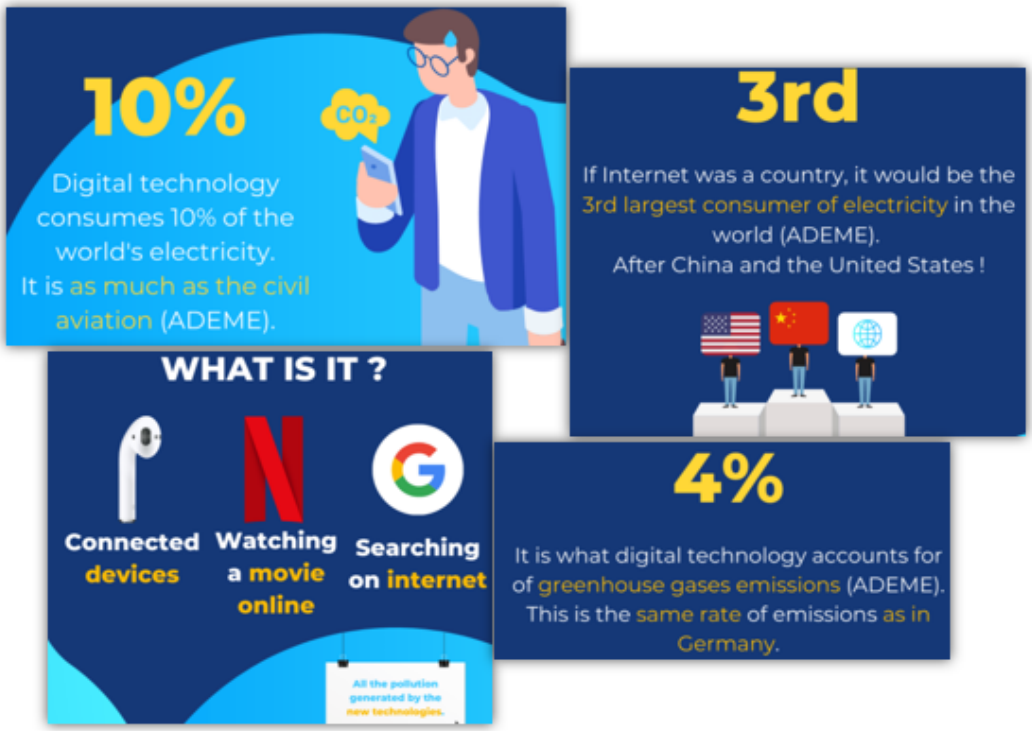
PLAGIARISMA

PROTECTING THE ENVIRONMENT

Technologies are spreading into all aspects of our lives via smart devices, internet of things, augmented reality and data profiling. Children's lives have become digital by default, with digital technologies the taken-for-granted means of playing, communicating with family, doing schoolwork, hanging out with friends.

DIGITAL POLLUTION

Children must understand from early stages of education that every single search query, every streamed song or video and every email sent, billions of times over all around the world - it all adds up to an ever-increasing global demand for electricity, and to rising CO2 emissions too. Our increasing reliance on digital tools has an environmental impact that's becoming increasingly harder to ignore.



https://ayruu.com/en/news/digital-pollution-the-new-challenge-of-tomorrow

Every time we browse, communicate, meet online, upload images or stream videos a small amount of carbon dioxide is emitted and in the last year or so this has increased beyond expectations. These carbon emissions are a result of the data storage and the network infrastructure needed to support the internet and store the content we access, which are incredibly energy intensive.

PROTECTING THE ENVIRONMENT

According to statistics from the UN, an estimated 50 million tons of electronic waste are generated worldwide each year - and the trend is rising.

https://www.mercurynews.com/

Children must understand that just because we can't physically see or touch the data that we're sending and receiving all over the globe, it actually involves huge energy consumption that is constantly growing.

The smart devices we use are often produced under exploitative and environmentally harmful conditions and, at the end of their far too short lives, they end up as electronic waste which pollute the environment and can be dangerous for people's health.

People must be aware that the life cycle of our electronic and IT devices (smartphones, tablets, laptops) does not start when they buy or receive them, and does not end when people get bored or replaced them. The life cycle of such products begin with the extraction of the raw materials used for its production and packaging.

Recycling e-waste not only helps to conserve energy, but it also recycles natural resources like copper, gold, silver and aluminum. Many of the metals used in our gadgets are rare earth metals that are in limited supply. When they are recycled they can be reused instead of having to mine for new supplies. That also helps prevent air and water pollution.

Learning about sustainability from early stages of education helps develop sustainable patterns of behavior that can become sustainable lifestyle habits in the future, such as being careful with scare resources. Young children can learn to be water and energy savers, good recyclers, and to think about the amount of waste we all generate on a daily basis.

If children start their environmental education at school they will learn that the fate of the planet is in their hands and they will learn how to use resources wisely and bring their contribution for protecting the environment .

REFERENCES

https://www.schooleducationgateway.eu , 28.11.2019

https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids, 30.11.2019

https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope ,30.11.2019

https://epthinktank.eu/2018/10/28/victims-of-cyberbullying-what-europe-does-for-you/ 2.12.2019