DATA PRIVACY, ETHICS & SECURITY

#R2AS03

What is it?

The activity sheets #R2AS03 and #R2AS04 aim to address general themes in order to engage teachers and students in a discussion on the different ethical and security issues related to data sharing and promotion.

Modalities

Going further activity.

Duration

1h30

Level of difficulty

Basic

Material

- No specific material needed
- Access to the internet will be a plus to check the resources proposed in the activity sheet

LEARNING OBJECTIVES

- Basics of data privacy and exposure of private data when acting on the digital ecosystem

This activity sheet is part of the Let's STEAM project funded with support from the European Commission through the Erasmus + Strategic Partnership programme. Its content reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

DATA PRIVACY, ETHICS & SECURITY

STEP 1 - ORIENTATE

20 min.

It is possible that you have heard that Google spy on us. Have you ever searched how can it be? What have you found? Some years ago, research revealed that Google was spying through non-encrypted routers. You can find some more information here and here!

DISCUSS WITH YOUR PEERS WHAT YOU THINK

Do you know what is a router for?
Where have you seen a router?
Have you ever heard what is encryption?
Can you imagine what is it for?
Can you imagine what kind of information can be accessible in WiFis detected?

You can perform a small brainstorming exercise with your peers.

STEP 2 - CONCEPTUALISE

15 min.

As you can imagine, all information that is shared through the router can be in the form of an email, social networks, or many other things you do when you use the Internet.

THINK ABOUT IT A BIT

What do you use the internet for? What searches do you do? What pages do you visit?
Have you noticed that on many pages it appears a request for you to accept cookies?
Do you usually accept cookies? Why?
Can you imagine what type of information is shared (and can be stored about you), when surfing the internet?
Do you "like" that all this information about you can be stored? Can you imagine the potential risks of storing it?
Have you read in detail the privacy policy of data protection of some of the websites you usually use?
Which other Internet resources have you used in the previous Let's STEAM modules?
Are there some resources which you would like to review its privacy policy?

Discuss with your peers and try to sot the type of information that can be stored about you when you use the Internet, based on the potential risk of it.

STEP 3 - INVESTIGATE

How do you know which type of information is shared about you and what risk might lead to? To have a first approach, try to search your full name on the Internet and see what results come up (include search in online gaming and social media accounts).

- **Do you think that the results reflect who you are and/or what you do? How? Try to search for one or two close friends.**
- **Do you think that the results reflect who they are and/or what they do? How?**
- **Have you contributed to providing more information about them on the Internet? How?**
- **Which information do you think your friends have shared about you?**

Discuss these issues with your peers. You can update the list of information and the risks you previously identified with new topics if is necessary. With a **group of 3-4 peers**, try to identify **10 best practices or actions to reduce the risks of sharing different types of information** and keep privacy in personal data. *For example: Which actions could we undertake to keep our information private? (Is it better to have a public profile on social media or a private profile? // download any app from the AppStore // navigate on the internet logged in on your Google account...).* You can relate to the list you previously did and define different practices according to the level of sensitivity of the information.

Afterwards, your group will merge with another small group. **Read the best practices designed by the other members of the group**. Try to merge and make a common list of 10 best practices by:

- **Identifying which practices/actions are similar between groups and merge them.**
- **Discussing the relevance of the different practices/actions trying to order them from more relevant to less relevant.**

Additionally, you can repeat the same merging with another group work so you can finally have a common list for the big group of trainees.

STEP 4 - CONCLUDE

Discuss with the whole group the most important actions/best practices to reduce the exposure of private data.

WILL YOU TRY TO IMPLEMENT THEM FROM NOW ON?