**SAFETY RULES ONLINE**

**Module 4 – Health Literacy and Use of Interactive services:   
the Social Media**

This is a brief list of rules to keep in mind for a positive experience on online interactions, correct use of devices and surfing the net in a safe environment.

**SAFETY WITH YOUR DEVICES**

* Lock your devices 🡪 choose your preferred way to unlock them (fingerprint, password, pin, etc.)
* Use a strong password 🡪 a strong password should be at least 12 characters long and unique. One of the easiest ways to remember a long and complex password without having to write it anywhere, is making it a sentence, even best if it is in your own local dialect!
* Learn how to use privacy settings in your devices

**SAFETY WITH APPS AND TABLET/SMARTPHONE**

* + Check the permission an app requires before downloading them (e.g., permission to access your contact lists or photos)
  + Do not provide any personal data unless the website or app are legitimate in asking it (e.g. national and official Health Care Systems and related apps)
  + Do not respond to any message that says your device has a virus, even if they say they are Microsoft, Apple, Android etc.
  + Do not click on links in emails automatically, especially if they sound alarming, like “you won a lottery” “you won a smartphone” or “your bank account has been violated”. Usually these alarming emails are used by cybercriminals to commit fraud and steal your data.

**SAFETY ON SOCIAL MEDIA**

* + Learn how to use privacy settings of any social media you use.
  + Do not share pictures of children (e.g. nephews and nieces) or underaged persons (e.g. a class of student, a volunteer group) without the consent of their parents.
  + Don't share any sensitive data.
  + Once you post something online, it can be downloaded or forwarded to other people. Always keep this in mind before sharing anything!
  + Think before posting: a provocative post, insults, or vulgar content, or even intimate details (e.g. about being hospitalized) may exposed you to problems later on (e.g. being fired from your job after a racist or homophobic post).
  + Be aware of fake news: before sharing something you found online, remember to check the source (e.g. website with misspelled name of reputable social media usually share fake news). Also, remember that, just because something sparks rage in you, is horrible or make you feel “right” it does not mean it is true.
  + Be aware of hate speech: Learn how to recognise hate speech and avoid using it. Also, learn how to report an offensive post or comment, and how to block a user that is targeting you with hate speech (e.g. via private messages, public comments, etc.)
  + Be nice to other people. You can disagree with another people’s opinion, and you can express it without offending them.
  + If you wish to meet someone in real life that you “met” online, do it in a public place or go with a friend. People may lie about their identity.

**S****AFETY ON SHOPPING, BANKING AND DONATING ONLINE**

* + Shop only on reputable online website. If you do not know them, you can search or ask around.
  + Use only credit or debit cards, do not send money or cash.
  + Before donating to a charity, check if they are legitimate.
  + Do not share your banking account access accounts and password.

This material related to the Elily project, made by the beneficiaries jointly or individually in any form and using any means, reflects only the author’s view, and the National Agency and the European Commission are not responsible for any use that may be made of the information it contains.