Media literacy program and material for adult educators

ANNEX 6:
Secure use of social networks

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

Project APRICOT:
Attentive parental education for wise being and co-being in changing times

This intellectual output has been conceived and developed by the Strategic Partnership in APRICOT project under the coordination and responsibility of *Šiuolaikinių didaktikų centras*/ *Modern Didactics Centre* (LT).

Thanks to all partners for their precious contributes:

Apricot Training Management Ltd. (UK)
ItF Institut Kassel e.V. – Frauencomputerschule (DE)
Planeta Ciencias (ES)

Editorial coordinator: Daiva Penkauskienė

Authors: Hilary Hale, Beate Hedrich, Betül Sahin, Alejandra Goded, Anca Dudau, Daiva Penkauskienė

Editorial Board: Sophy Hale, Seda Gürcan, Konrad Schmidt, Cihan Sahin, Josafat Gonzalez Rodriguez, Roc Marti Valls, Virgita Valiūnaitė

Month/ Year: November 2021

9.6 Annex 6: Secure use of social networks

1. Different email addresses and secure passwords

If possible, you should use different email addresses for the accounts of the different social networks. This makes it more difficult to be compiled into a comprehensive profile with the information you give on the respective pages. Freemail accounts can be used for the different email addresses. These accounts should be called up occasionally so that they remain activated. When choosing a provider, care should be taken to ensure that the provider does not let the email address expire and reassign it to a new user. Otherwise, there is a risk that another user will take over this email address and thus gain access to the associated social network.

The use of different and secure passwords for the individual services such as Facebook or Twitter is also recommended. The following applies to the password: the longer, the better. It should be at least eight characters long, should not appear in the dictionary and consist of upper- and lower-case letters as well as special characters and numbers. A password manager, such as keepass.info, can make it easier to handle different passwords. Never give your password to third parties.

2. Two-Factor Authentication

With two-factor authentication, security is further enhanced. This means: The first factor is a strong password (category knowledge). As a second factor, a security token, i.e. a hardware component such as a key, a smart card or a special USB stick, is used for additional authentication (category possession). An SMS sent by the provider can also be used. This provides much better protection for the user account. For unauthorized access third parties would need both factors, both knowledge of the password and ownership of the device.

3. Caution when installing apps, add-ons or plug-ins

Many social networks allow you to install third-party applications, such as games. However, online criminals also create such applications and exploit them to gain access to the profile. Before installation, the provider and sources should be checked for trustworthiness.

4. Special caution for mobile use

Social networks are often used via mobile devices such as smartphones or tablets. Operators or third-party providers provide apps for this purpose. These apps often use sensitive data available on the mobile device, such as address book, photos, videos or location information. In addition, the mobile device is usually automatically registered with the social network afterwards. If the device is lost, this can be exploited by the finder or

thief misrepresenting themselves as the owner. For this reason, try not to store passwords on mobile devices and instead of using the app, log on and off directly from the social network website.

5. Contact request

Identity theft is one of the risks of the digital age. Contact requests should be accepted with caution. If dubious requests are received from acquaintances, always check the trustworthiness of these messages. As a matter of principle, only include people known from the real world in your friends or contact list. Unknown persons could have malicious intentions. "Fake friends" can assume a foreign identity with the help of assumed or fake accounts and possibly use them for criminal offences or illegal online business.

6. Weigh up every click on links or buttons beforehand

Online criminals use social networks to lure users with postings or links in chats to prepared websites. These websites are then used to access data or infect devices with malware. An innocent click can cause an installation of malware on your device. This malware can, for example, switch on the device's camera unnoticed, record conversations through the microphone, or query the location. Address book, photos or videos stored on the device can fall into unauthorized hands.

7. Protect privacy

Every social network offers numerous privacy settings. These settings can be used to show your profile only to friends and allow postings. The close integration of social network operators with other Internet services should be considered. This allows a very comprehensive profile of the user to be created. You should occasionally conduct an online search for yourself or family members to find out what information can be found about you. You should also regularly check the security settings of the social media accounts you use and pay attention to the links to other accounts. Social media providers may change these settings on their own initiative.

Do not give any personal information on the network. Once a piece of information is published on the Internet, it is very difficult or impossible to delete it.

8. Report cyberstalking and hate comments

- Report persons who harass or insult others to the operator of the social network. The operators can investigate and delete dubious profiles.
- In the case of obvious or suspected offences, seek advice from the police.
- Inform those affected and, if necessary, file a complaint.

9. Delete account

If an account is no longer in use, back up your data and then delete the account.

Read data protection regulations and general terms and conditions (AGB)

10. Rights and Responsibilities

Social networks are operated by profit-oriented companies, which are mostly financed by advertising. The terms and conditions provide information on how the provider handles your personal data and how this data is passed on to the advertising industry. Before creating a profile, please read the terms and conditions and the data protection regulations thoroughly.

Some social networks grant themselves rights of use to your publications. This means, for example, that the rights of use for photos and videos are transferred to the operator of the social network. In addition, it is quite common that granted rights of use remain even if the user has left the network and deleted the profile. So, think twice before publishing. Care should also be taken to ensure that the rights of third parties are not infringed by posting pictures, texts or videos.

Social networks also have rules of conduct (netiquette) that must be observed.

Netiquette refers to rules that are taken for granted by the majority of people. Almost every forum and every website, chat room etc. has its own netiquette. However, the guidelines are largely the same.

- First read, then think, then post
- keep text short
- Observe legal regulations
- Be polite and tolerant
- No excessive use of the Shift key or punctuation marks such as exclamation marks
- No verbal attacks
- Note spelling
- Use punctuation marks
- Saying "thank you" won't hurt anyone.
- No spam and no novels
- No excessive use of smileys
- No discrimination, sexist or racist slogans
- Do not publish personal data, telephone numbers or advertising

In forums it is often regulated in netiquette that the search function is used first before asking a question. In most cases, this prevents a question that has already been asked from being rewritten again and again.

Depending on the portal, blog etc. the list of rules can vary. As a rule, Netiquette is also used on Facebook, in emails and in other places where you can write your own texts and comments on the net.

11. Personal attacks and cyberbullying

Social media, messenger services and other apps enable or facilitate cyberbullying and cyberstalking. They often offer not only the platforms on which the bullying or stalking takes place, but also make private information of the users publicly accessible.

12. Cyberbullying

Cyberbullying is the deliberate insulting, threatening, exposing or harassing of other persons through the Internet and mobile phone services over a period of time. The perpetrator ("bully") looks for a victim who is unable to or has difficulties defending themselves against the attacks. The perpetrator uses this imbalance of power and thus leads the victim into social isolation.

Cyberbullying takes place in social networks, in video portals and via smartphones through instant messaging applications such as WhatsApp, annoying phone calls etc. The bully usually acts anonymously, so the victim does not know from whom the attacks come from. The opposite is true for children and young people, who usually know each other from their "real" personal environment. The victims therefore almost always suspect who might be behind the attacks.

13. Difference between cyberbullying and bullying

Cyberbullying differs in some ways from bullying in the real world.

- Cyber bullying does not end after school or work. Because cyber-bullies can attack over the Internet 24 hours a day. They can even stalk you at home.
- The level of cyberbullying is greater than bullying in the real world because
  - the audience is unmanageably large
  - Content spreads extremely fast
  - Contents that have long been forgotten can always come back to the public
  - Bullies can act anonymously:

The offender does not show themselves directly to their victim. Not knowing who the perpetrators are can frighten and unsettle a victim.

The effect on the victim is not immediately apparent?

The perpetrator does not see the victim's reactions to a hurtful statement or to a disrespectful image and therefore may not be fully aware of the extent of the effects of their attacks.

14. Facets of bullying

Bullying has different facets:

- **Chicane**: Repeatedly sending offensive and hurtful messages via email, SMS, instant messenger or in chats.
- **Slander / rumours:** Spreading rumours through the Internet and mobile phone services to a large group of people.
- **Exposing:** Information that was originally made available in confidence to a specific person is sent to others to compromise the victim.
- **Exclusion/Ignore**: Deliberate exclusion from social activities, groups, chats, etc.

15. Influence of cyberbullying on web culture

The Internet is leading to massive changes in the way people communicate with each other. On the one hand, it is a positive development that you can always be reached without any problems or quickly check what your friend has written. Or which photo has just been posted. On the other hand, however, negative tendencies can also be observed, which this new "online communication culture" brings with it.

16. Fast pace of life

The transmission speed of the Internet has become faster and the mobile Internet is also constantly improving its performance. Information reaches the user in ever shorter intervals. However, users have also adapted to this. Communication is becoming faster and more restless. One day offline means: the following day, a number of messages from friends, acquaintances or colleagues are on the computer or smartphone.

However, this speed also leads to posts, pictures or videos being spontaneously shared and sent. Not only positive, but also snapshots or derogatory comments that are unfavourable for a person. This information spreads very quickly via various services to an unmanageably large group of people.

17. Anonymity & distance

The anonymity favours a disinhibited online communication. Anyone who travels anonymously on the Internet may expect hardly any negative consequences for their actions. Moreover, the direct reaction of the other party cannot be seen via online communication, except for video chat. The user is therefore often unable to assess how his or her statements are received by other users because he or she cannot see how the other person reacts in facial expressions and gestures. Since one does not meet the other person face to face, it is easy to hurt other feelings online.

18. Excessive sharing of personal information

Social networks and many services, such as WhatsApp, Twitter, Ask.fm etc. rely on the fact that users share many things with others. Children and teenagers are easily tempted to reveal a lot about themselves, because they want to test out how to reach their peers. However, the feedback from others on posted photos, videos and other contributions is not always positive and the user gets discredited and harassed by their self-portrayal to others.

19. Friends versus acquaintances

Using social networks and instant messengers, new acquaintances can be made quickly and easily. These are then immediately added on Facebook, WhatsApp and Co. Over time, more and more contacts accumulate, coming from a wide variety of contexts. It becomes more and more difficult to keep an overview. But it is important to know who can read the posts, see the photos, because not everything is suitable for all contacts.

Many social networks offer users the option to sort their contacts into different groups. The posts that the user uploads can be shared specifically for the individual groups (friends, acquaintances, etc.). In this way, unpleasant reactions to personal contributions from strangers can be avoided.

20. Tips for parents

How can parents know that their child is being bullied?

Cyberbullying can be detected and combated in its early stages. If you notice that the child suddenly changes its behaviour, help is needed. Signs of this are when the child:

- behaves with restraint,
- loses the desire to communicate,
- has drastically changed online usage,
- isolates itself from the outside world,
- reacts aggressively,
- has many excuses or inexplicable physical complaints,
- his/her appearance is oriented towards role models and beauty ideals
- or downplays his/her own situation.

If these symptoms occur, parents should talk to their child immediately, because the beginnings of cyberbullying must be urgently tackled to prevent damage. If the child is already being massively bullied, it is always advisable to consult an expert. Online help can be found at Bündnis gegen Cybermobbing e.V. - Mobbing Internet/Netz ((https://www.buendnis-gegen-cybermobbing.de) and Klicksafe

(https://www.klicksafe.de/themen/kommunizieren/cyber-mobbing).

21. How can parents help their children?

It is important to actively approach bullying victims, talk about their problems and provide initial emotional support. However, parents should also seek the advice and opinion of an expert. For example, the free telephone counselling hotline. This hotline can be reached anonymously 24 hours a day and has appropriately trained contact persons. It is also important to face the child's problems and to act openly. One should be open to family and friends and discuss and take further steps together.

22. How can you protect yourself against cyberbullying?

There is no guarantee that you will not become a victim of cyberbullying. Simple but effective methods can be used to reduce the danger. As always, the same applies here:

- never reveal too much of your private life on the Internet,
- Control privacy settings and friends closely,
- Think about who or what you do on the Internet,
- never talk publicly about worries and problems on the Internet,

Again, "knowledge is power!"

Parents should sensitize their children to the handling of cyberbullying by talking openly with their child about bullying and going through the different variants. A very important point is that parents give their child the security of knowing that they can always talk to them.