MODULE 2: Digital Content Creation

Unit 4 : Protecting personal data and privacy

Some useful points of information

Media literacy guides the researcher through the responsible way of internet usage. One of the key elements is the respect of personal identity. Taking photos during the event keeps the memories but can violate someone's privacy. Before the event make sure to collect the agreement from the participants to have their photos taken. Keep in mind that if the participants are under 18 years old, the parent's permission or the permission of the official representative is needed.

This topic is extremely important when taking group photos. Based on privacy law, community members can ask to blur their photo or to delete the photo. This right should be respected.

If a data leakage took place, it is always possible to request the removal of information and to apply for the reimbursement if the rights were violated.

EU information rules ensure the safety of your own information at whatever point they are gathered – for instance, when you purchase something on the web, you can request the information about the operation. These standards apply to providers that offer services in the EU, like Facebook or Amazon, at whatever point these organizations solicitation or re-utilize the individual information of people in the EU.

In order to keep control over information keep an eye on your passwords and use a key generator to make sure that all your passwords are unique. Log out of social media every time you use public computers to make sure that no one is able to have access to your personal data.

In spite of the fact that cybercriminals have become progressively more refined in their actions, there are ways you can spot suspicious connections and protect your digital privacy.

Don't follow suspicious links that are sent to your email.

One of the ways to minimize data traction by third-parties is to browse in the **Incognito mode in your browser**. This mode helps to minimize the information shared with searching engines. See https://www.computerworld.com/article/3356840/how-to-go-incognito-in-chrome-firefox-safari-and-edge.html

Suspicious links threaten the profiles and can cause a potential digital assault, explicitly known as a **phishing**. The objective of a phishing assault is to utilize email to trick the user to follow the link and as a result to get private information. Phishing is considerably more focused to an individual client or business. The suspicious connections in these messages are quite often masked to engage with the user via web search tools that individuals utilize each day.

Some useful links

Safer Internet Day https://www.saferinternetday.org/en-GB/supporters/european-schoolnet

European Commission on data protection https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

EU data privacy and protection https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection

Guidelines on Children’s Data Protection in an Education Setting https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b

Your Europe: data protection https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm

GDPR for schools and teachers https://www.schooleducationgateway.eu/en/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm

Education for online safety https://www.betterinternetforkids.eu/documents/167024/902349/SIF2009EurydiceReport.pdf/4d3936f7-68bc-4c02-8960-4242db917120