LESSON PLAN

★ — ★ ★

Privacy, my most precious possession

5.1. You cannot say everything to everyone

Short Activity Title	You cannot say everything to everyone
Author	Evangelia Kontopidi, Greece
Topic	Privacy, my most precious possession
Competences	Social and civic competences / Communication in the mother tongue / Digital competence
Level	☑ Easy ☑ Intermediate ☐ Difficult
Age Group	13-15 years
Duration	Two-three lessons of 45 min each (depending on how students present their outcomes).
Aim of this lesson	• Develop students' awareness of privacy and data protection. • Help students discover ways to protect their personal data and maintain positive digital footprints. • Encourage students to work together on a collaborative task. • Encourage students to study resources, analyse material and present conclusions in a creative way.
Introduction	In this lesson students *explore* the meaning of the terms: privacy, personal data, sensitive personal data; *watch* a video in order to think about the possible implications and impact of what they post online; *study* and analyse material related to privacy and digital footprints on proposed websites, and *create tips* for protecting their privacy and online reputation.
Tools	(a) Internet-connected digital devices such as computers, laptops, tablets, etc. (b) Web browser (c) Search engine (d) Optional: Web 2.0 applications (Wordle, Scratch, Tricider, Voki, Google Forms or SurveyMonkey), presentation software (Prezi, Microsoft PowerPoint and Google Slides) (Registration required for Google Forms, Google Slides and Prezi)
Process	
Step 1 – (10 minutes)	**Investigate – discuss** Consider key terms: privacy, personal data and sensitive personal data. Write these words on the board. Ask students to think about definitions / examples for these words. Check in advance whether information on these key terms exists in the national Data Protection Authority (DPA) website. If this is the case, encourage students to search the corresponding website (http://goo.gl/eblbFv.)

	Brainstorm a list of words related to the above key terms, i.e. *personal data*: information which allows individuals to be identified, i.e., name, home or email address, telephone number (mobile or fixed), credit card number, date of birth, image or voice, etc.; *sensitive personal data*: political opinions, religious beliefs, physical or mental health condition, etc.; *privacy*: someone's right to keep their personal matters and relationships secret.
Step 2 – (10 minutes)	**Watch - Listen - Discuss** Challenge students to think what might happen if someone shares too much of their personal data with the rest of the world. Use a video such as this http://youtu.be/T6ulH2bWCnY to stimulate interest in the topic and encourage thinking. Furthermore, you could present students with two facts: (a) People's digital footprints (pictures, online published content, etc.) play a major role in companies' recruitment procedures; (b) Cyberbullying occurs more frequently on sites visited by large numbers of teenagers. Personal data protection helps to prevent cyberbullying. More information at http://www.e-abc.eu/en/about-bullying/. Establish a list of reasons why students should purposely limit access to their private information.
Step 3 – (25 minutes)	**Collaborate - Investigate** At this point, students should have realised that privacy is very important and therefore this lesson is personally meaningful to them, i.e. (a) They should use social media, responsibly, and (b) They should protect their online reputation. It is time now for students to focus on investigating specific ways to accomplish these two aims. The EU NET ADB project http://goo.gl/TyAJh2 reports that 92 per cent of adolescents aged 14-17 years old who participated in the study (in 7 European countries), are members of at least one social networking site. Ask students to work in small groups of two or three and use the internet to investigate privacy policies and settings on social networking sites such as Facebook, Google+, YouTube or Instagram. Students should look for answers to questions such as: What features/tips does the service provide to help people protect their privacy? • How do I update my profile/privacy settings? • How do I remove content posted without my consent? • How do I choose who can see photos and other things I post? • How do I delete something I have posted?

	Assign each group to study one of the following pairs of resources. Alternatively, groups make their own choice that best suits their interests and social networking activities. • Facebook Privacy Basics https://www.facebook.com/about/basics/ • Facebook Help Centre - Privacy https://www.facebook.com/help • Google+ Safety Center - Managing your digital reputation for teens https://support.google.com/plus/topic/2404767 • Google+ Teen Safety Guide - General Tips http://goo.gl/6MI93L • Google+ Safety Center - Privacy resources http://goo.gl/7WzbQG • YouTube Policy Center - Protecting your privacy http://goo.gl/6ajG4U • YouTube Safety Center - Teen Safety http://goo.gl/H2oxRG • Instagram Help Center https://help.instagram.com/ • Instagram Privacy and Safety Tips http://goo.gl/iBHDeZ • Online Reputation Checklist http://goo.gl/hvnfZM After studying content on the suggested websites, each team formulates a report with five top tips for protecting privacy or managing online reputation.
Step 4 – (45 minutes)	**Practice – Produce - Present** Each group reads its report aloud. The class should agree on five things they will change to improve their report and make a declaration for display on a classroom wall and/or for the school newsletter or website. In addition, if more time can be dedicated to the activity, consider alternative ways for groups to present their results and conclusions. These alternative options enable students to use their creativity and practise digital skills. (a) Make use of the social voting tool Tricider and create a 'tricision' on the topic: "Data protection, privacy, online reputation: share your thoughts and ideas". Prepare in advance the 'tricision' (its creation takes only a few minutes), give students the link and ask them to write their own key message on the topic. Then students vote for the two ideas they like the most (they are not allowed to vote for their own idea). The student whose idea gets the most votes is the winner! (A sample 'tricision' can be found on http://goo.gl/XmzeEF.) (b) Groups create Vokis (speaking avatars) and record their tips. Vokis are presented in the class and can also be embedded on the school website for future reference. (c) Groups create posters using an application or software they are familiar with. A simple model poster can be found on http://goo.gl/pg7DQM (the model poster was created with MS PowerPoint. In the Page Setup Group, slide was set to "A4 paper" size and to "Portrait" orientation. Finally, the work was saved as a PDF file.)

	(d) Groups generate word clouds from text that is related to their findings and conclusions using a Web 2.0 application such as Wordle or Tagxedo. A simple model word cloud can be found on http://goo.gl/wXJ3nq. It was created with Wordle using the following text: http://goo.gl/ofc3Jw. (e) Groups formulate questions based on their findings and create their own 'privacy quiz' for their peers. Questions should not be too obvious or too difficult. Groups exchange quiz sheets and do the test. Alternatively, groups could use an online quiz generator such as Google Forms or SurveyMonkey. Also Scratch provides resources for creating a question/answer system. A model Scratch quiz on privacy can be found at http://goo.gl/EGXdyU. This last Scratch activity allows students to enhance their understanding of the privacy topic by 'playing' with each other's Scratch quizzes. However, it might take longer to be implemented and it is intended for students with some experience in programming with Scratch. [Scratch is an easy to learn and use programming language. Based on the inGenious project (http://www.ingenious-science.eu/web/guest/home), the use of Scratch in teaching can help students develop creativity, computational thinking and active engagement in class.]
Follow up options	**Pop up - Tools - Tips** For school or at home, give students handouts of the online reputation checklist http://goo.gl/hvnfZM and ask them to go through the five steps, which could help them manage and maintain positive digital footprints. Discuss with your class and organise Data Protection Day http://goo.gl/3322q4 (January 28th) and organise with students some awareness activities for the school and for the local community.
Links	• Oversharing: Think Before You Post - Video http://goo.gl/FT4OYK • Digital Footprint - Video http://goo.gl/QkBR4j • Irish Data Protection Authority Resource on Privacy http://goo.gl/uv1vUF • Think before you share guide (poster form) http://goo.gl/PcH0yd • The microsite "Young Citizens" under the Greek Data Protection Authority website (for Greek teachers only) http://goo.gl/hRQx • Good policies for handling personal data on Facebook http://goo.gl/MDmnJr video on saferinternet.gr website (for Greek teachers only)