STIAEM

Slow Tech Innovation

AI, Ethics and

New Teaching Methods

Cyber Hygiene Protocols: Anonymised Accounts and Profiling Prevention

Co-funded by the European Union

2025-1-IT02-KA220-SCH-000365213

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them... Project reference code: 2025-1-IT02-KA220-SCH-000365213

Università di Foggia

Studi Umanistici, Lettere, Beni Culturali, Scienze della Formazione

İSTANBUL - ESENLER

İLÇE MİLLİ EĞİTİM MÜDÜRLÜĞÜ

1474

STIAEM

Slow Tech Innovation AI, Ethics and New Teaching Methods

Co-funded by the European Union

2025-1-IT02-KA220-SCH-000365213

eduOpen



CC BY-NC-SA 4.0 International
This license requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, for noncommercial purposes only. If others modify or adapt the material, they must license the modified material under identical terms.

Università di Foggia
Studi Umanistici, Lettere, Beni Culturali, Scienze della Formazione

OER 5.2.2: Cyber Hygiene Protocols: Anonymised Accounts and Profiling Prevention
Reference Module: Module 5 - Safety, Privacy and Sustainability
Related Video-Pill: Video 5.2: Terms of Use (ToS) & Account Protection
Authoring partner: Rhodes Evening High School - Greece
Topic / Thematic Focus: Cyber hygiene protocols, anonymised accounts and profiling prevention

Introduction and Learning Objectives

This resource completes the path of video-pill 5.2 and accompanies OER 5.2.1. Its subject is cyber-hygiene practices: the set of simple and systematic habits with which the school protects accounts, devices and digital identities. There are two focuses: the use of anonymised or class accounts and the prevention of commercial profiling of students.
The text connects to DigComp 3.0 (Cosgrove & Cachia, 2025), competences 4.1 «Protecting devices» and 4.2 «Protecting personal data and privacy», and to the Slow Tech model (Patrignani & Whitehouse, 2019). The legal references are the GDPR (arts. 4, 22) and the DSA (arts. 26, 28).
By the end of the reading, the teacher will be able to:

- adopt safe management practices for school accounts, including class and pseudonymised accounts;
- recognise what profiling is and what protections the legal order offers with respect to automated decisions;
- protect students' data by avoiding the entry of personal information into generative AI tools.

1. Why cyber hygiene is a teaching practice

Cyber hygiene evokes images of complicated passwords and security software. At school, however, it is above all a matter of habits: how accesses are created and safeguarded, where data ends up, what is written inside an automatic tool. These are everyday gestures that, if neglected, open breaches in the protection of students; if practised regularly, they become part of the implicit curriculum of digital citizenship.
The first principle is informational sobriety, already encountered with minimisation: the less data circulates, the smaller the risk surface. The second is the separation of profiles: distinguishing what is personal from what is didactic. The third is traceability: knowing which tools we use and with which data.
An often neglected aspect is the physical environment: shared devices, interactive whiteboards, laboratory computers retain traces of accesses. Cyber hygiene therefore also includes simple material habits: closing the session, not saving credentials on shared devices, checking that temporary files are deleted. These are gestures that do not require technical skills, but attention and consistency, and that it is useful to turn into explicit classroom rules.

2. Anonymised accounts and class accounts

The most effective practice for reducing risks is not to associate students' data with personal identities when it is not necessary. One can use pseudonyms (one student, one code), group accounts for collaborative activities, or institutional accounts managed by the school that do not require personal details from commercial platforms.

This approach has a legal basis in the principle of minimisation and purpose limitation (GDPR, art. 5), but it also has an educational value: students learn that digital identity is not a commodity to be offered in exchange for a free service. An anonymised account is, in miniature, a lesson in aware citizenship.

Linked to account management are good access practices: strong passwords that differ for each service, two-step verification where available, attention to shared devices and closing the session. On the organisational level, it is advisable to define who in the school manages the credentials and how they are revoked at the end of the year.

On the organisational level, it is useful to distinguish three levels of accounts: teachers' personal accounts, which remain as such and must not be used to give students access; the school's institutional accounts, managed centrally and revocable; class accounts, created for a single activity and then decommissioned. Keeping this distinction avoids confusion and reduces the risk that data from different students accumulate in the same profile. At the end of the year, the decommissioning of class accounts is an integral part of digital cleanup.

3. Recognising profiling

The second focus is profiling, that is, the automatic construction of a person's profile starting from their data. The GDPR gives a precise definition of it.

«'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements» (GDPR, art. 4, par. 1, point 4).

Recognising profiling is the first step to defending against it. When a platform «suggests» content, orders information or personalises advertising, it is applying a profile. The DSA prohibits profiled advertising aimed at minors and the use of special categories of data for advertising purposes (DSA, arts. 26.3 and 28.2): these are prohibitions that the teacher can invoke in choosing tools.

A further step concerns fully automated decisions that produce effects on the student.

«The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her» (GDPR, art. 22, par. 1).

And the protection is strengthened for minors: the European legislator specifies that measures of this kind should not concern a minor (GDPR, recital 71). At school the consequence is clear-cut: no decision affecting a student's path - an admission, an assessment, a guidance choice - should be left to the machine alone. A recommendation system, however, is useful as support: the difference lies in keeping the decision in human hands.

Recognising profiling also requires knowing how to read interfaces. A feed that orders content «for you», an advertisement that seems to guess your tastes, a friend suggestion: these are

all signs that a system is building a profile. For the school this translates into a concrete question: does the service we use order and personalise content based on students' behaviour? If the answer is yes, we must check what is done with that data and whether the personalisation is compatible with the didactic purpose.
Research by Obar and Oeldorf-Hirsch (2018) shows that users tend to ignore the privacy notices they accept. The guidelines of the European Data Protection Board illustrate how to apply the protections to automated decisions and profiling (EDPB/WP29, 2018).

4. Personal data and generative AI tools

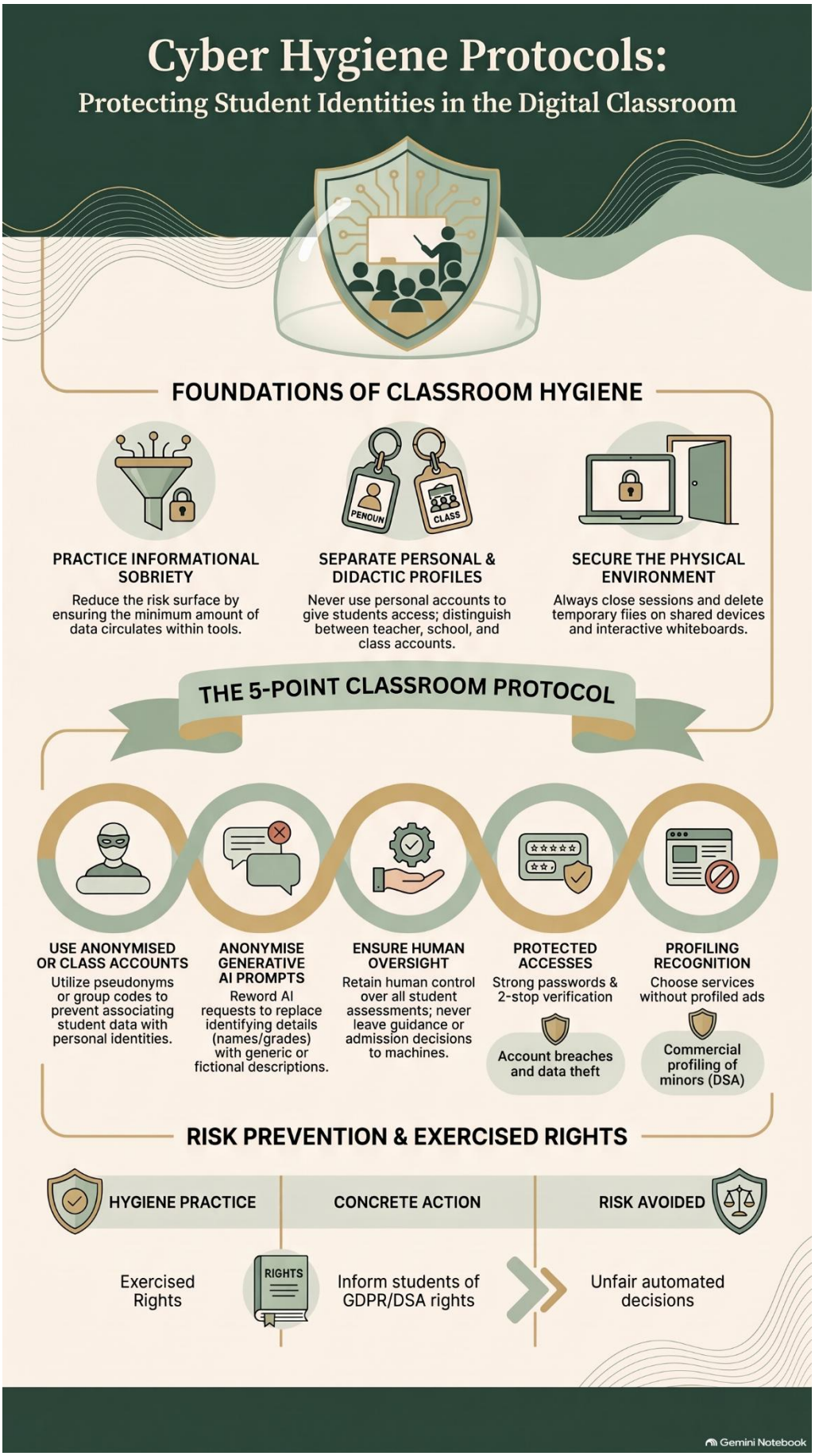
A specific chapter of cyber hygiene concerns chatbots and assistants based on generative AI. Entering a student's name, a grade, a diagnosis or a photograph into a prompt means processing personal data, often with tools that retain and reuse them. The practical rule is simple: identifying data do not go into requests to AI. If a concrete case is needed, fictional examples are used or the details are anonymised.
This protects the students but also educates them: showing how «clean» requests are formulated is an effective way of teaching respect for privacy in the daily use of AI. This is connected to the protection provided by the AI Act for high-risk systems, which must be able to be supervised by competent persons during use (AI Act, art. 14).
A useful expedient concerns the wording of requests. Before writing a prompt concerning a classroom situation, it is worth asking: does it contain names, health data, assessments, elements that make it possible to identify a person? If so, it is reworded by replacing the identifying details with generic descriptions. This discipline, besides protecting students, has formative value: it teaches that the quality of a request to AI also depends on respect for the limits we set ourselves.
A final element concerns the education of students: cyber hygiene is not transmitted with a prohibition, but with an understanding of the why. Explaining what a profile is and what it means to leave a digital trace helps students to make autonomous choices also outside school. It is in this autonomy, more than in surveillance, that the most lasting protection of their digital identity lies.

5. A cyber-hygiene protocol for the classroom

From the practices described, a five-point protocol is derived. First: prefer class accounts or pseudonyms for didactic activities. Second: protect accesses with strong passwords and two-step verification. Third: do not enter personal data into generative AI tools. Fourth: recognise and limit profiling, by choosing services that do not practise it on minors. Fifth: inform and enforce students' rights, always maintaining human intervention in decisions that concern them.
The following table links each practice to the risk it prevents.
For the protocol to hold over time, it is advisable to integrate it into a recognisable routine: at the start of the year the accounts and access rules are defined, along the way the practices on data are recalled, at the end of the year the accounts are decommissioned and materials no longer needed are deleted. Consistency counts more than sophistication: simple but practised cyber hygiene is worth more than complex measures applied once and forgotten.

Hygiene practice	Objective	Concrete action	Risk avoided
Class/pseudonym accounts	Do not associate data with identities	Use codes or group accounts	Exposure of the student's identity
Protected accesses	Prevent unauthorised access	Strong passwords and two-step verification	Breach of accounts and data
Data out of *prompts*	Do not process personal data with AI	Use fictional or anonymised examples	Unlawful processing of personal data
Profiling recognised	Reduce commercial personalisation	Prefer services without profiled advertising	Profiling of minors (prohibited by the DSA)
Rights exercised	Maintain human control	Inform and provide for human intervention	Automated decisions affecting students

Visual Scaffolding



Conclusions and Metacognitive Reflection Prompts

This resource has translated information security into everyday cyber hygiene: anonymised or class accounts, protected accesses, no personal data in prompts, recognition of profiling and protection of students' rights. The foundation is twofold: the GDPR, which defines profiling and limits automated decisions, and the DSA, which prohibits profiled advertising aimed at minors. The message for the teacher is that the protection of digital identity is built with small repeated gestures, not with great exceptional measures.

To transfer these core ideas to one's own practice, the following reflection prompts are proposed:

- In your digital activities, could you replace a personal account with a class or pseudonym account?
- Which personal data habitually appear in the texts you entrust to an AI tool, and how could you anonymise them?
- How would you explain to a class, with an example, the difference between personalised advice and an automated decision?

Technical Metadata Sheet

Metadata Field	Specification / Parameter Value
Identifier	OER 5.2.2
Title	Cyber Hygiene Protocols: Anonymised Accounts and Profiling Prevention
Creator	Rhodes Evening High School - Greece
Description	Complementing OER 5.2.1, the resource addresses cyber-hygiene practices: the simple, systematic habits with which schools protect accounts, devices and digital identities. Its two focuses are the use of anonymised or class accounts and the prevention of profiling, together with the protections the legal order offers against automated decisions. The practical focus is a cyber-hygiene protocol for the classroom and the protection of student data in generative AI tools.
Keywords	cyber hygiene; anonymised accounts; class accounts; profiling; automated decisions; account protection; student data; classroom protocol
Language	EN (English)
Affiliation	Rhodes Evening High School - Greece
Contributor	STIAEM Transnational Scientific Board (peer review, Rhodes validation protocol)
Media Format	Text; Infographics
Genre	Training Manual; Educational Guide
URL	
Citation	Cosgrove, J., & Cachia, R. (2025). DigComp 3.0: European digital competence framework (Fifth edition). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/0001149 European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). Official Journal of the European Union, L 277, 1-102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 12.7.2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870 European Data Protection Board / Article 29 Working Party. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01). https://ec.europa.eu/newsroom/article29/items/612053
Educational Level	Secondary School
Associated Module / MOOC Video Lesson	Module 5 - Safety, Privacy and Sustainability / Video 5.2 - Terms of Use (ToS) & Account Protection
Learning Objectives	adopt safe management practices for school accounts, including class and pseudonymised accounts; recognise what profiling is and what protections the legal order offers with respect to automated decisions; protect students' data by avoiding the entry of personal information into generative AI tools.
Rights	Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)
Date Available	14/09/2026
Date Modified	

References and Webography

Cosgrove, J., & Cachia, R. (2025). DigComp 3.0: European digital competence framework (Fifth edition). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/0001149

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). Official Journal of the European Union, L 277, 1-102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 12.7.2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870

European Data Protection Board / Article 29 Working Party. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01). https://ec.europa.eu/newsroom/article29/items/612053