SURVEY OF CYBERSECURITY COVERAGE IN EUROPEAN COMMISSION DIGITAL COMPETENCE FRAMEWORKS, SELF-ASSESSMENT TOOLS & GUIDES

SuperCyberKids
Deliverable D2.1, Annex 3

Call: ERASMUS-EDU-2022-PI-FORWARD
Type of Action: ERASMUS-LS
Project No. 101087250

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

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project ref. number	101087250
Project title	SCK - SuperCyberKids
Document title	SCK D2.1 Annex 3 - Survey of Cybersecurity Coverage in EC Digital Competence Frameworks, Self-Assessment Tools & Guides
Document Type	Deliverable (Annex)
Document version	07 (28/07/2023)
Previous version(s)	06 (24/07/2023)
Planned date of delivery	July, 2023 (M7)
Language	English
Dissemination level	Public
Number of pages	67
Partner responsible	CNR (WP2 Leader)
Author(s)	Jeffrey Earp, CNR; Chiara Fante, CNR; Flavio Manganello, CNR.
With contributions by	
Keywords	cybersecurity, digital competence framework, digital competence, digital capacity, self-assessment, European Union, European Commission, digital education, blended learning, bullying, cyberbullying

Survey of cybersecurity coverage in European Commission digital competence frameworks, self-assessment tools & guides

About this document

This document surveys a set of digital competence/digital capacity frameworks, self-assessment tools and guides that the European Commission (EC) has developed over recent years to help further education in the digital age and to support the development of digital skills. The primary purpose of this survey is to provide essential input (along with other desktop studies and field investigations) for defining the "**SuperCyberKids Skills Framework" (SCKSF).** This is being developed in SuperCyberKids, a European research project co-funded under the EC's Erasmus+ programme. SuperCyberKids has a mandate to produce a game-based cybersecurity education ecosystem dedicated first and foremost to children aged 8 to 13 and their teachers/educators, but also to other actors in the education community and beyond. The SCKSF-supported ecosystem should help those involved to acquire and develop competences in cybersecurity and cybersecurity education through playful engagement with game-based cybersecurity learning content, teaching materials, and processes. In parallel with its primary mission, this survey also provides a comparative overview of the different initiatives that the EC has launched in the framing and self-assessment of digital competence/digital capacity in education across Europe (and now beyond). So this document may also help various actors in the European education landscape get a better grasp of the constantly expanding and evolving opportunities that the EC is providing for digital competence development and how it approaches the provision of that support.

Co-funded by the European Union

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.

Index

1. **INTRODUCTION** p.4

2. **EC DIGITAL COMPETENCE FRAMEWORKS & SELF-ASSESSMENT TOOLS**

2.1. [DigComp 2.2] - The Digital Competence Framework for Citizens p.7

2.2. [DigCompOrg] - European Framework for Digitally Competent Educational Organisations p.21

2.3. [SELFIE] - Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies p.27

2.4. [DigCompEdu] - European Framework for the Digital Competence of Educators p.33

2.5. [SELFIEforTEACHERS] p.40

3. **EC GUIDES TO BLENDED LEARNING IN THE COVID-19 ERA**

3.1. Blended Learning for High Quality and Inclusive Primary and Secondary Education – Handbook p.49

3.2. Blended learning in school education – guidelines for the start of the academic year 2020/21 p.49

4. **EC PUBLICATIONS FOCUSING ON CYBERSECURITY MATTERS**

4.1. [ECSF] - European Cybersecurity Skills Framework p.53

4.2 [What can schools do about bullying?] - EC factsheet p.56

5. **DISCUSSION & FINAL CONSIDERATIONS** p.59

5.1. Coverage of the cybersecurity domain p.59

5.2 Description/reification of competences in the digital education & cybersecurity fields p.63

5.3. Competence Proficiency Positioning & Grading p.63

5.4 SuperCyberKids Skills Framework (SCKSF) & EC digital competence initiatives: opportunities p.65

6. **REFERENCES** p.66

Co-funded by the European Union

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.

Co-funded by the European Union

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.

1. INTRODUCTION

The European Commission (EC) has set out its strategy to further education in the digital age and support of digital skills development in "Digital Education Action Plan (2021-2027) – Resetting education and training for the digital age" (European Commission, 2020). The Action Plan (DEAP) clearly states that this endeavour is tightly intertwined with issues of cybersecurity:

> "*With computers and algorithms mediating many daily activities, it is important to educate people at all ages about the impact of digital technology on well-being and the way technology systems work. This is instrumental to developing an understanding of the risks and opportunities of digital technology and encouraging healthy, safe and meaningful uses of digital technology*". (p.9 - emphasis added)

The recent European Parliamentary Research Service briefing paper "Progress on the European Commission's 2021-2027 digital education action plan" (March, 2023) also highlights this link, stressing concerns about children's digital welfare in particular:

> *"Members warned that it is still difficult to assess the impact of digital technologies on education, and underlined the importance both of implementing prevention programmes to improve children's safety online and of addressing cybersecurity threats. Members deemed basic digital skills essential …".* (p.9 - emphasis added)

With this in mind, this survey focuses specifically on **how and to what degree the considered set of EC digital competence frameworks, self-assessment tools and guides addresses topics within the domain of cybersecurity**. The primary purpose is to provide input (along with other sources) for the definition of the "SuperCyberKids Skills Framework" (SCKSF) being developed in Work Package 2 of SuperCyberKids, a European project co-funded under the EC's Erasmus+ programme. In addition, the document may also prove useful as an **overview and comparison of different EC initiatives dedicated to the framing and self-assessment of digital competence/digital capacity in the education domain**.

As illustrated in Fig. 1, this survey considers **five major conceptual frameworks and related self-assessment tools**: The Digital Competence Framework for Citizens (DigComp); the Digital Competence Framework for Digitally Competent Educational Organisations (DigCompOrg); SELFIE (Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies); The European Framework for the Digital Competence of Educators (DigCompEdu); and SELFIEforTEACHERS.

The survey also examines **two EC guides to blended learning in the COVID-19 era** ("Blended learning for high quality and inclusive primary and secondary education – Handbook"; "Blended learning in school education – guidelines for the start of the academic year 2020/21"). These have been included in the survey in the light of the boom in Emergency Remote Teaching and blended learning triggered by response to the COVID-19 pandemic. This crisis clearly brought the issue of digital competence/digital capacity into sharp focus, and hence also considerations about cybersecurity.

The survey also examines **two EC publications more specifically focused on cybersecurity matters**, namely ECSF - European Cybersecurity Skills Framework (by the European Union Agency for Cybersecurity - ENISA), and the EC factsheet "What can schools do about bullying?". These documents have been included in the survey as recent examples of EC initiatives specifically devoted (or closely related) to cybersecurity matters, spotlighting EC attention to the question.

Each of the initiatives listed above is described by way of (i) an introductory table with summary information about the initiative in question; (ii) a graphic representation of its domain scope; (iii) a brief explanation of how the framework/tool/guide contents are structured and presented; and (iv) extracts from the framework/tool/guide that pertain to cybersecurity matters.

Following examination of the above surveyed initiatives, some final considerations are made, including about how those initiatives and the "SuperCyberKids Skills Framework" (SCKSF) documented in SuperCyberKids Deliverable 2.1 may gain mutual benefits that help further ongoing efforts to achieve the DEAP objectives.

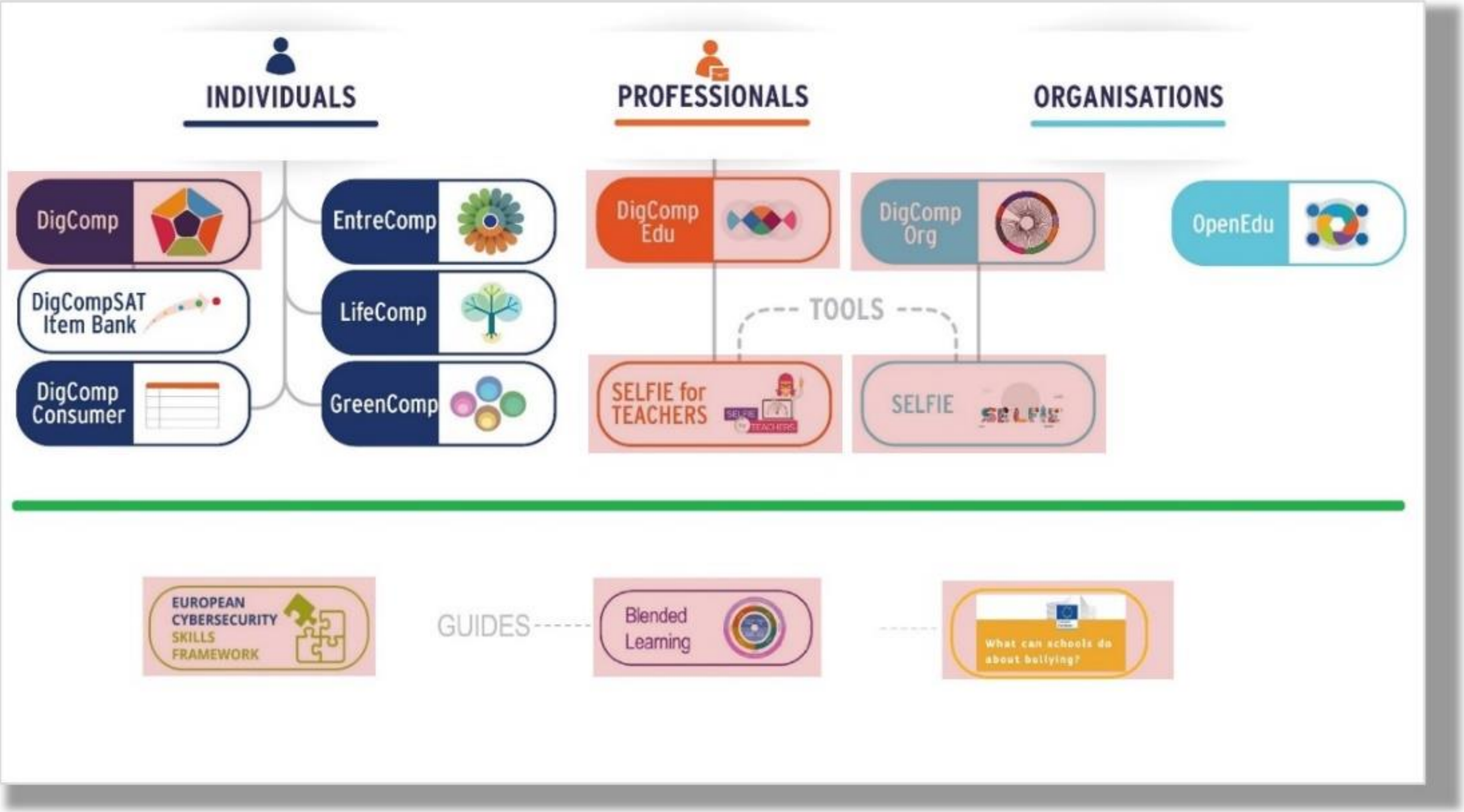


Fig. 1 - surveyed EC digital competence frameworks, self-assessment tools and guides (those highlighted in pink are addressed in this study). [1]

[1] Image from Vuorikari, R., Kluzer, S., and Punie, Y. (2022): emphasis added. Identified cybersecurity-related content in these initiatives is highlighted in pink throughout in this document

2. EC digital competence frameworks & self-assessment tools

2.1. **[DigComp 2.2]** - The Digital Competence Framework for Citizens

framework	The Digital Competence Framework for Citizens (DigComp)
versioning	DigComp (2013), DigComp 2.0 (2016), DigComp 2.1 (2017), DigComp 2.2 (2022)
description	DigComp is the EC-published digital competency framework for citizens/individuals. The first version (2013) was a landmark work providing a basis for subsequent EC efforts for furthering digital competency and capacity in education. These efforts have seen development of frameworks and self-assessment tools that are devoted to a range of targets and application domains, and intended for use by different stakeholders, a number of which feature in this survey.
primary target	citizens/individuals
organisation & structure	Five macro competence areas grouping 21 competences. For each competence, the framework proposes: a title and short descriptor; "*I can…*" statement-items that reify the competence at eight progressive proficiency levels; lists of knowledge, skills and attitudes that exemplify the competence; uses cases that illustrate the competence in both professional and educational settings ("learning scenario") and at different proficiency levels.
cybersecurity coverage	One of the framework's five macro competence areas, SAFETY, is dedicated to cybersecurity related matters. SAFETY comprises four individual competences, three of which specifically address cybersecurity issues. In addition, the macro competence area COMMUNICATION & COLLABORATION contains two competences, Netiquette and Managing Digital Identity, which have implications related to cybersecurity matters.

framework (cont.)	The Digital Competence Framework for Citizens (DigComp)
EC platform	https://joint-research-centre.ec.europa.eu/digcomp_en
main EC publications	• **DigComp 2.2** Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415 [© European Union 2022. Creative Commons Attribution 4.0 International (CC BY 4.0) - https://creativecommons.org/licenses/by/4.0/] • **DigComp 2.1** Carretero, S.; Vuorikari, R. and Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use, EUR 28558 EN, doi:10.2760/38842 [© European Union, 2017. "*The reuse of the document is authorised, provided the source is acknowledged and the original meaning or message of the texts are not distorted*."] • **Guide** European Commission, Joint Research Centre, Punie, Y., Pujol Priego, L., Carretero, S.et al., DigComp into action, get inspired make it happen – A user guide to the European Digital Competence framework, Punie, Y.(editor), Carretero, S.(editor), Vuorikari, R.(editor), Publications Office, 2018, https://data.europa.eu/doi/10.2760/112945 [© European Union, 2018 – "*Reuse is authorised provided the source is acknowledged.*"]

Domain scope of DigComp 2.2 framework

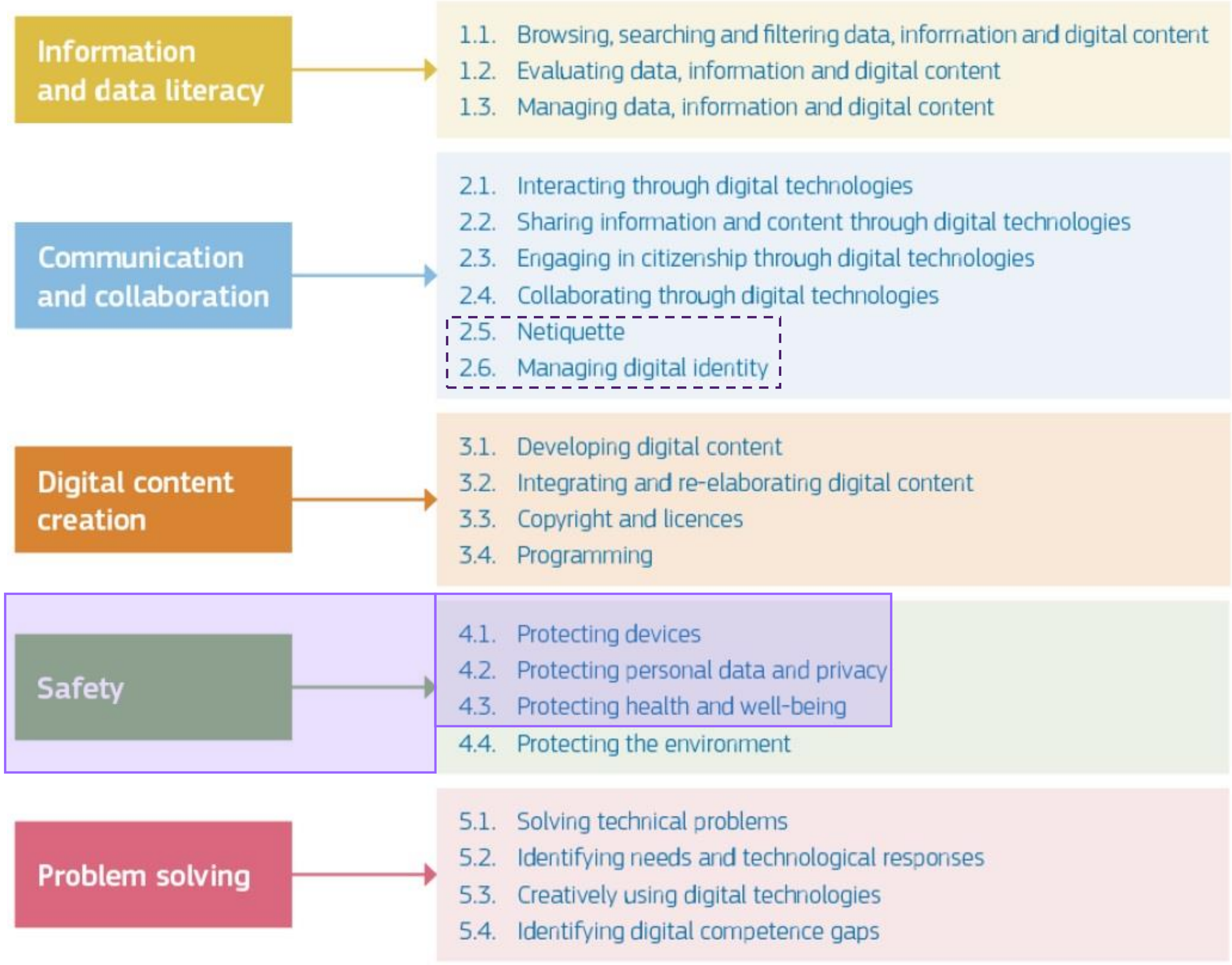

Information and data literacy
1.1. Browsing, searching and filtering data, information and digital content
1.2. Evaluating data, information and digital content
1.3. Managing data, information and digital content
Communication and collaboration
2.1. Interacting through digital technologies
2.2. Sharing information and content through digital technologies
2.3. Engaging in citizenship through digital technologies
2.4. Collaborating through digital technologies
2.5. Netiquette
2.6. Managing digital identity
Digital content creation
3.1. Developing digital content
3.2. Integrating and re-elaborating digital content
3.3. Copyright and licences
3.4. Programming
Safety
4.1. Protecting devices
4.2. Protecting personal data and privacy
4.3. Protecting health and well-being
4.4. Protecting the environment
Problem solving
5.1. Solving technical problems
5.2. Identifying needs and technological responses
5.3. Creatively using digital technologies
5.4. Identifying digital competence gaps

Fig. 2 - The five digital competence macro areas of the DigComp 2.2 framework[2]

[2] Image from Vuorikari, R., Kluzer, S., and Punie, Y. (2022): emphasis added.

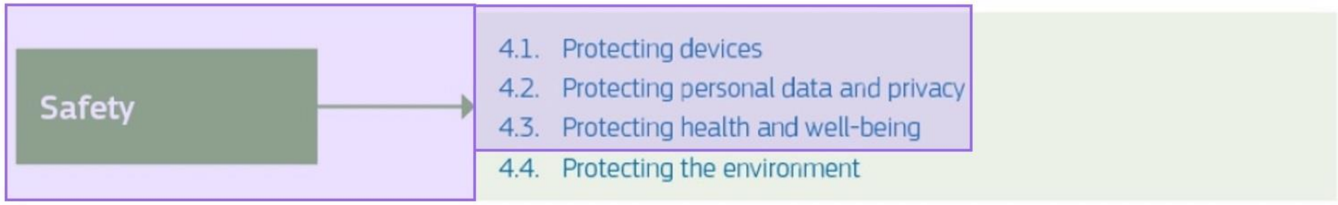
Organisational structure of DigComp 2.2 framework

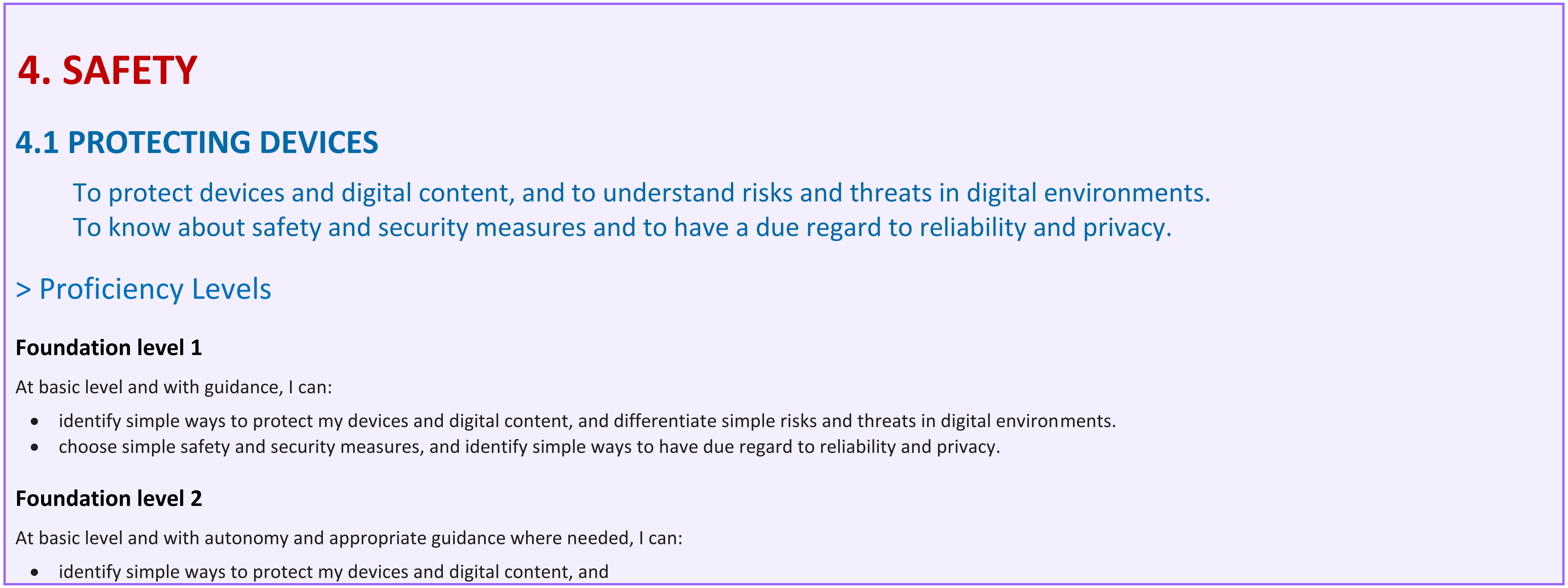
[The DigComp 2.2 Framework has five “structural dimensions”]

- **Dimension 1** [competence areas forming the domain of digital competence]
- **Dimension 2** [individual competences within the competence area, each with a title and descriptor]
- *> Dimension 3* [“I can …” statements that reify the competence at eight progressive proficiency levels: Foundation (levels 1 & 2), Intermediate (3 & 4), Advanced (5 & 6),
  Highly Specialised (7 & 8)]
- *Dimension 4* [List of knowledge, skills and attitudes applicable to each competence]
- *Dimension 5* [“I can …” use cases illustrating competence application in both professional and education settings, and at the four main proficiency categories:
  Foundation, Intermediate, Advanced, Highly Specialised]

Coverage of cybersecurity domain in DigComp 2.2 framework

[The DigComp 2.2 macro competence area SAFETY covers four specific competences, three of which are dedicated to cybersecurity matters.]


Safety
4.1. Protecting devices
4.2. Protecting personal data and privacy
4.3. Protecting health and well-being
4.4. Protecting the environment



4. SAFETY

4.1 PROTECTING DEVICES

To protect devices and digital content, and to understand risks and threats in digital environments.
To know about safety and security measures and to have a due regard to reliability and privacy.

> Proficiency Levels

Foundation level 1

At basic level and with guidance, I can:

- identify simple ways to protect my devices and digital content, and differentiate simple risks and threats in digital environments.
- choose simple safety and security measures, and identify simple ways to have due regard to reliability and privacy.

Foundation level 2

At basic level and with autonomy and appropriate guidance where needed, I can:

- identify simple ways to protect my devices and digital content, and

[3] Image extracted from Vuorikari, R., Kluzer, S., and Punie, Y. (2022): emphasis added.

- differentiate simple risks and threats in digital environments.
- follow simple safety and security measures.
- identify simple ways to have due regard to reliability and privacy.

Intermediate level 3

On my own and solving straightforward problems, I can:

- indicate well-defined and routine ways to protect my devices and digital content, and
- differentiate well-defined and routine risks and threats in digital environments, and
- select well-defined and routine safety and security measures.
- indicate well-defined and routine ways to have due regard to reliability and privacy

Intermediate level 4

Independently, according to my own needs, and solving well-defined and non-routine problems, I can:

- organise ways to protect my devices and digital content, and
- differentiate risks and threats in digital environments.
- select safety and security measures.
- explain ways to have due regard to reliability and privacy.

Advanced level 5

As well as guiding others, I can:

- apply different ways to protect devices and digital content, and
- differentiate a variety of risks and threats in digital environments.
- apply safety and security measures.
- employ different ways to have due regard to reliability and privacy.

Advanced level 6

At advanced level, according to my own needs and those of others, and in complex contexts, I can:

- choose the most appropriate protection for devices and digital content, and
- discriminate risks and threats in digital environments.
- choose the most appropriate safety and security measures.
- assess the most appropriate ways to have due regard to reliability and privacy.

Highly Specialised level 7

At highly specialised level, I can:

- create solutions to complex problems with limited definition that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments.

- integrate my knowledge to contribute to professional practice and knowledge and guide others in protecting devices.

Highly Specialised level 8

At the most advanced and specialised level, I can:

- create solutions to solve complex problems with many interacting factors that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments.
- propose new ideas and processes to the field.

Examples of Knowledge, Skills and Attitudes

Knowledge

- Knows that using different strong passwords for different online services is a way to mitigate the negative effects of an account being compromised (e.g. hacked).
- Knows about measures to protect devices (e.g. password, fingerprints, encryption) and prevent others (e.g. a thief, commercial organisation, government agency) from having access to all data.
- Knows about the importance of keeping the operating system and applications (e.g. browser) up-to-date, in order to fix security vulnerabilities and protect against malicious software (i.e. malware).
- Knows that a firewall blocks certain kinds of network traffic, aiming to prevent different security risks (e.g. remote logins).
- Aware of different types of risks in digital environments, such as identity theft (e.g. someone committing fraud or other crimes using another person's personal data), scams (e.g. financial scams where victims are tricked into sending money), malware attacks (e.g. ransomware).

Skills

- Knows how to adopt a proper cyber-hygiene strategy regarding passwords (e.g. selecting strong ones difficult to guess) and managing them securely (e.g. using a password manager).
- Knows how to install and activate protection software and services (e.g. antivirus, anti-malware, firewall) to keep digital content and personal data safer.
- Knows how to activate two-factor authentication when available (e.g. using one-time passwords, OTP, or codes along with access credentials).
- Knows how to check the type of personal data an app accesses on one's mobile phone and, based on that, decides whether to install it and configures the appropriate settings.
- Able to encrypt sensitive data stored on a personal device or in a cloud storage service.
- Can respond appropriately to a security breach (i.e. an incident that results in unauthorised access to digital data, applications, networks or devices, the leaking of personal data such as logins or passwords).

Attitudes

- Vigilant not to leave computers or mobile devices unattended in public places (e.g. shared workplaces, restaurants, trains, car backseat).
- Weighs the benefits and risks of using biometric identification techniques (e.g. fingerprint, face images) as they can affect safety
- in unintended ways. If biometric information is leaked or hacked, it becomes compromised and can lead to identity fraud.
- Keen to consider some self-protective behaviours such as not using open Wi-fi networks to make financial transactions or online banking.

Use Cases

Employment Scenario: Use of a Twitter account to share information on my organization
Advanced level 5

- I can protect the corporate Twitter account using different methods (e.g. a strong password, control the recent logins) and show new colleagues how to do it.
- I can detect risks like receiving tweets and messages from followers with false profiles or phishing attempts.
- I can apply measures to avoid them (e.g. control the privacy settings).
- I can also help my colleagues to detect risks and threats while using Twitter.

Learning Scenario: Use of the school's digital learning platform to share information on interested topics
Advanced level 5

- I can protect information, data and content on my school's digital learning platform (e.g. a strong password, control the recent logins).
- I can detect different risks and threats when accessing school's digital platform and apply measures to avoid them (e.g. how to virus-check attachments before downloading).
- I can also help my classmates to detect risks and threat while using the digital learning platform on their tablets (e.g. controlling who can access the files).

4.2 PROTECTING PERSONAL DATA AND PRIVACY

To protect personal data and privacy in digital environments. To understand how to use and share personally identifiable information while being able to protect oneself and others from damages. To understand that digital services use a "Privacy policy" to inform how personal data is used.

> Proficiency Levels

Foundation level 1

At basic level and with guidance, I can:

- select simple ways to protect my personal data and privacy in digital environments,
- identify simple ways to use and share personally identifiable information while protecting myself and others from damages.
- identify simple privacy policy statements of how personal data is used in digital services.

Foundation level 2

At basic level and with autonomy and appropriate guidance where needed, I can:

- select simple ways to protect my personal data and privacy in digital environments
- identify simple ways to use and share personally identifiable information while protecting myself and others from damages.

- identify simple privacy policy statements of how personal data is used in digital services.

Intermediate level 3

On my own and solving straightforward problems, I can:

- explain well-defined and routine ways to protect my personal data and privacy in digital environments, and explain well-defined and routine ways to use and share personally identifiable information while protecting myself and others from damages.
- indicate well-defined and routine privacy policy statements of how personal data is used in digital services.

Intermediate level 4

Independently, according to my own needs, and solving well-defined and non-routine problems, I can:

- discuss ways to protect my personal data and privacy in digital environments, and
- discuss ways to use and share personally identifiable information while protecting myself and others from damages.
- indicate privacy policy statements of how personal data is used in digital services.

Advanced level 5

As well as guiding others, I can:

- apply different ways to protect my personal data and privacy in digital environments,
- apply different specific ways to share my data while protecting myself and others from dangers.
- explain privacy policy statements of how personal data is used in digital services.

Advanced level 6

At advanced level, according to my own needs and those of others, and in complex contexts, I can:

- choose the more appropriate ways to protect personal data and privacy in digital environments, and
- evaluate the most appropriate ways of using and sharing personally identifiable information while protecting myself and others from damages.
- evaluate the appropriateness of privacy policy statements on how personal data are used.

Highly Specialised level 7

At highly specialised level, I can:

- create solutions to complex problems with limited definition that are related to protecting personal data and privacy in digital environments, using and sharing personally identifiable information protecting self and others from dangers, and privacy policies to use my personal data.
- integrate my knowledge to contribute to professional practice and knowledge and guide others in protecting personal data and privacy

Highly Specialised level 8

At the most advanced and specialised level, I can:

- create solutions to solve complex problems with many interacting factors that are related to protecting personal data and privacy in digital environments, using and sharing personally identifiable information protecting self and others from dangers, and privacy policies to use my personal data.
- propose new ideas and processes to the field.

Examples of Knowledge, Skills and Attitudes

Knowledge

- Aware that secure electronic identification is a key feature designed to enable safer sharing of personal data with third parties when conducting public sector and private transactions.
- Knows that the “privacy policy” of an app or service should explain what personal data it collects (e.g. name, brand of device, geolocation of the user), and whether data are shared with third parties.
- Knows that the processing of personal data is subject to local regulations such as the EU’s General Data Protection Regulation (GDPR) (e.g. voice interactions with a virtual assistant are personal data in terms of the GDPR and can expose users to certain data protection, privacy and security risks). (AI)

Skills

- Knows how to identify suspicious e-mail messages that try to obtain sensitive information (e.g. personal data, banking identification) or might contain malware. Knows that these emails are often designed to trick people who do not check carefully and who are thus more susceptible to fraud, by containing deliberate errors that prevent vigilant people clicking on them.
- Knows how to apply basic security measures in online payments (e.g. never sending a scan of credit cards or giving the pin code of a debit/payment/credit card).
- Knows how to use electronic identification for services provided by public authorities or public services (e.g. filling-in your tax form, applying for social benefits, requesting certificates) and by the business sector, such as banks and transport services.
- Knows how to use digital certificates acquired from certifying authorities (e.g. digital certificates for authentication and digital signing stored on national identity cards).

Attitudes

- Weighs the benefits and risks before allowing third parties to process personal data (e.g. recognises that a voice assistant on a smartphone, that is used to give commands to a robot vacuum cleaner, could give third parties - companies, governments, cybercriminals - access to the data). (AI)
- Confident in carrying out online transactions after taking appropriate safety and security measures.

Use Cases

Employment Scenario: Use of a Twitter account to share information on my organization

Advanced level 6

- I can select the most appropriate way to protect the personal data of my colleagues (e.g. address, phone number) when sharing digital content (e.g. a picture) on the corporate Twitter account.
- I can distinguish between appropriate and inappropriate digital content to share it on the corporate Twitter account, so that my privacy and that of my colleagues are not damaged
- I can assess whether personal data are used on the Corporate Twitter appropriately according to the European Data Protection Law and Right to be Forgotten.

- I can deal with complex situations that can arise with personal data in my organisation while on Twitter, such as removing pictures or names to protect personal information in accordance with the European Data Protection Law and Right to be Forgotten.

Learning Scenario: Use of the school's digital learning platform to share information on interested topics
Advanced level 6

- I can distinguish between appropriate and inappropriate digital content to share it on my school's digital platform, so that my privacy and that of my classmates are not damaged.
- I can assess whether the way my personal data are used on the digital platform is appropriate and acceptable as regards my rights and privacy.
- I can select the most appropriate way to protect my personal data (e.g. address, phone number), before sharing it on the school's digital platform.
- I can overcome complex situations that can arise with my personal data and those of my classmates while on the digital education platform, such as personal data is not used in accordance to the "Privacy policy" of the platform.

4.3 PROTECTING HEALTH AND WELL-BEING

To be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies. To be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying). To be aware of digital technologies for social well-being and social inclusion.

> Proficiency Levels

Foundation level 1

At basic level and with guidance, I can:

- differentiate simple ways to avoid health risks and threats to physical and psychological well-being while using digital technologies.
- select simple ways to protect myself from possible dangers in digital environments.
- identify simple digital technologies for social well-being and social inclusion.

Foundation level 2

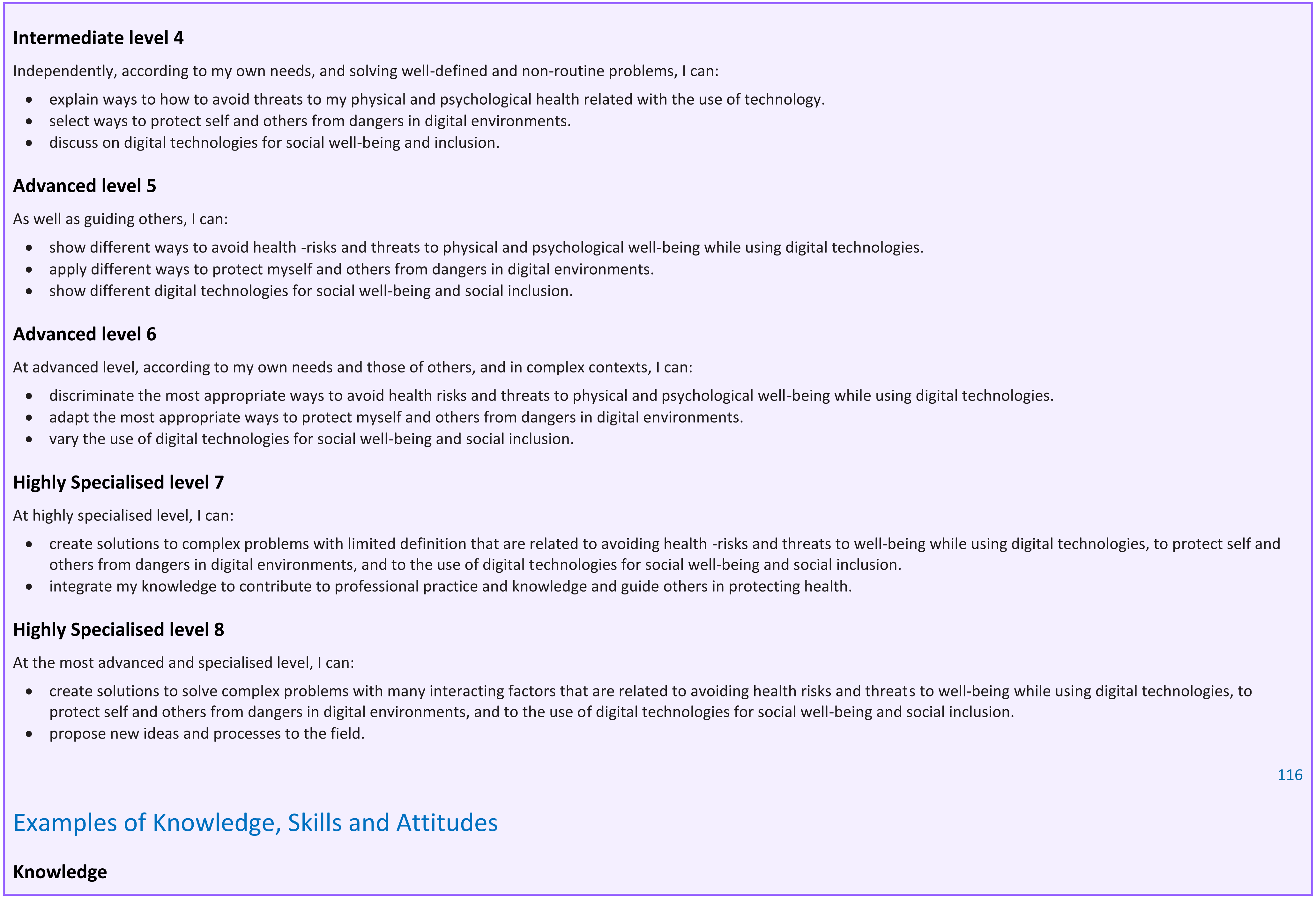
At basic level and with autonomy and appropriate guidance where needed, I can:

- differentiate simple ways to avoid health risks and threats to physical and psychological well-being while using digital technologies.
- select simple ways to protect myself from possible dangers in digital environments.
- identify simple digital technologies for social well-being and social inclusion.

Intermediate level 3

On my own and solving straightforward problems, I can:

- explain well-defined and routine ways to how to avoid health risks and threats to physical and psychological well-being while using digital technologies.
- select well-defined and routine ways to protect myself from dangers in digital environments.
- indicate well-defined and routine digital technologies for social well-being and social inclusion.



Intermediate level 4

Independently, according to my own needs, and solving well-defined and non-routine problems, I can:

- explain ways to how to avoid threats to my physical and psychological health related with the use of technology.
- select ways to protect self and others from dangers in digital environments.
- discuss on digital technologies for social well-being and inclusion.

Advanced level 5

As well as guiding others, I can:

- show different ways to avoid health -risks and threats to physical and psychological well-being while using digital technologies.
- apply different ways to protect myself and others from dangers in digital environments.
- show different digital technologies for social well-being and social inclusion.

Advanced level 6

At advanced level, according to my own needs and those of others, and in complex contexts, I can:

- discriminate the most appropriate ways to avoid health risks and threats to physical and psychological well-being while using digital technologies.
- adapt the most appropriate ways to protect myself and others from dangers in digital environments.
- vary the use of digital technologies for social well-being and social inclusion.

Highly Specialised level 7

At highly specialised level, I can:

- create solutions to complex problems with limited definition that are related to avoiding health -risks and threats to well-being while using digital technologies, to protect self and others from dangers in digital environments, and to the use of digital technologies for social well-being and social inclusion.
- integrate my knowledge to contribute to professional practice and knowledge and guide others in protecting health.

Highly Specialised level 8

At the most advanced and specialised level, I can:

- create solutions to solve complex problems with many interacting factors that are related to avoiding health risks and threats to well-being while using digital technologies, to protect self and others from dangers in digital environments, and to the use of digital technologies for social well-being and social inclusion.
- propose new ideas and processes to the field.

116

Examples of Knowledge, Skills and Attitudes

Knowledge

- Aware of the importance of balancing the use of digital technologies with non-use as an option, as many different factors in digital life can impact on personal health, wellbeing and life satisfaction.
- Knows signs of digital addictions (e.g. loss of control, withdrawal symptoms, dysfunctional mood regulation) and that digital addiction can cause psychological and physical harm.
- Aware that for many digital health applications, there are no official licensing procedures as is the case in mainstream medicine.
- Aware that some applications on digital devices (e.g. smartphones) can support the adoption of healthy behaviours by monitoring and alerting the user about health conditions (e.g. physical, emotional, psychological). However, some actions or images proposed by such applications could also have negative impacts on physical or mental health (e.g. viewing 'idealised' body images can cause anxiety).
- Understands that cyberbullying is bullying with the use of digital technologies (i.e. a repeated behaviour aimed at scaring, angering or shaming those who are targeted).
- Knows that the "online disinhibition effect" is the lack of restraint one feels when communicating online in comparison to communicating in-person. This can lead to an increased tendency towards online flaming (e.g. offensive language, posting insults online) and inappropriate behaviours.
- Aware that vulnerable groups (e.g. children, those with lower social skills and lack of in-person social support) are at a higher risk of victimisation in digital environments (e.g. cyber bullying, grooming).
- Aware that digital tools can create new opportunities for participation in society for vulnerable groups (e.g. older people, people with special needs). However, digital tools can also contribute to isolation or the exclusion of those who do not use them.

Skills

- Knows how to apply, for oneself and others, a variety of digital usage monitoring and limitation strategies (e.g. rules and agreements on screen-free times, delayed availability of devices for children, installing time limitation and filter software).
- Knows how to recognise embedded user experience techniques (e.g. clickbait, gamification, nudging) designed to manipulate and/or to weaken one's ability to be in control of decisions (e.g. make users to spend more time on online activities, encourage consumerism).
- Can apply and follow protection strategies to fight online victimisation (e.g. block receiving further messages from sender(s), not reacting/responding, forwarding or saving messages as evidence for legal procedures, deleting negative messages to avoid repeated viewing).

Attitudes

- Inclined to focus on physical and mental wellbeing, and avoid the negative impacts of digital media (e.g. overuse, addiction, compulsive behaviour).
- Assumes responsibility for protecting personal and collective health and safety when evaluating the effects of medical and medical-like products and services online, as the internet is awash with false and potentially dangerous information about health.
- Wary of the reliability of recommendations (e.g. are they by a reputable source) and their intentions (e.g. do they really help the user vs encourage to use the device more to be exposed to advertising).

Use Cases

Employment Scenario: Use of a Twitter account to share information on my organization
Highly specialised level 7

- I can create a digital campaign of possible health dangers of using Twitter for professional reasons (e.g. bullying, addictions, physical well-being) which can be shared and used by other colleagues and professionals on their smartphones or tablets.

Learning Scenario: Use of the school's digital learning platform to share information on interested topics
Highly specialised level 7

- I can create a blog on cyberbullying and social exclusion for my school's digital learning platform, which helps my classmates to recognise and face up to violence in digital environments

[other digital competences in DigComp 2.2 with (more or less direct) implications for cybersecurity]

2. COMMUNICATION AND COLLABORATION

2.5 NETIQUETTE

To be aware of behavioural norms and know-how while using digital technologies and interacting in digital environments. To adapt communication strategies to the specific audience and to be aware of cultural and generational diversity in digital environments.

<implications for appropriate/responsible/ethical online behaviour (e.g. avoidance and mitigation of cyberbullying>

2.6 MANAGING DIGITAL IDENTITY

To create, and manage one or multiple digital identities, to be able to protect one's own reputation, to deal with the data that one produces through several digital tools, environments and services.

< implications for privacy & personal data protection>

2.2. **[DigCompOrg]** - European Framework for Digitally Competent Educational Organisations

framework	The Digital Competence Framework for Digitally Competent Educational Organisations (DigCompOrg)
versioning	DigCompOrg (2015)
description	Foundational reference framework designed to foster "a pan-European approach to digital capacity" in educational organisations by guiding their "self-reflection on progress towards comprehensive integration and effective deployment of digital learning technologies". At policy level DigCompOrg is aimed at providing "a strategic planning tool and addressing fragmentation and uneven development across the Member States". DigCompOrg is the conceptual framework for the EC's self-evaluation tool for schools, **SELFIE** (see later entry)
primary target	Learning communities in primary, secondary, and VET schools, as well as higher education
organisation & structure	Seven macro competence areas ("thematic elements") grouping 15 competence areas ("sub-elements") common to all education sectors, plus room for inclusion of a sector-specific thematic element (e.g. VET), with its sub-elements and competences ("descriptors"). The seven predefined thematic elements and 15 sub-elements in the framework group a total of 74 competence items ("descriptors"). Each descriptor comprises a title-statement and an explanatory descriptor text.
cybersecurity coverage	Two competence areas ("Teaching and Learning Practices" & "Infrastructure") include descriptors (total = 4) that deal with cybersecurity related topics.
EC platform	https://joint-research-centre.ec.europa.eu/european-framework-digitally-competent-educational-organisations-digcomporg/digcomporg-framework_en
main EC publication	Joint Research Centre, Institute for Prospective Technological Studies, Devine, J., Punie, Y., Kampylis. Promoting effective digital-age learning – A European framework for digitally-competent educational organisations, Publications Office, 2015. https://dx.doi.org/10.2791/54070 [© European Union, 2015 ("*Reproduction is authorised provided the source is acknowledged.*")]

Domain scope of DigCompOrg framework

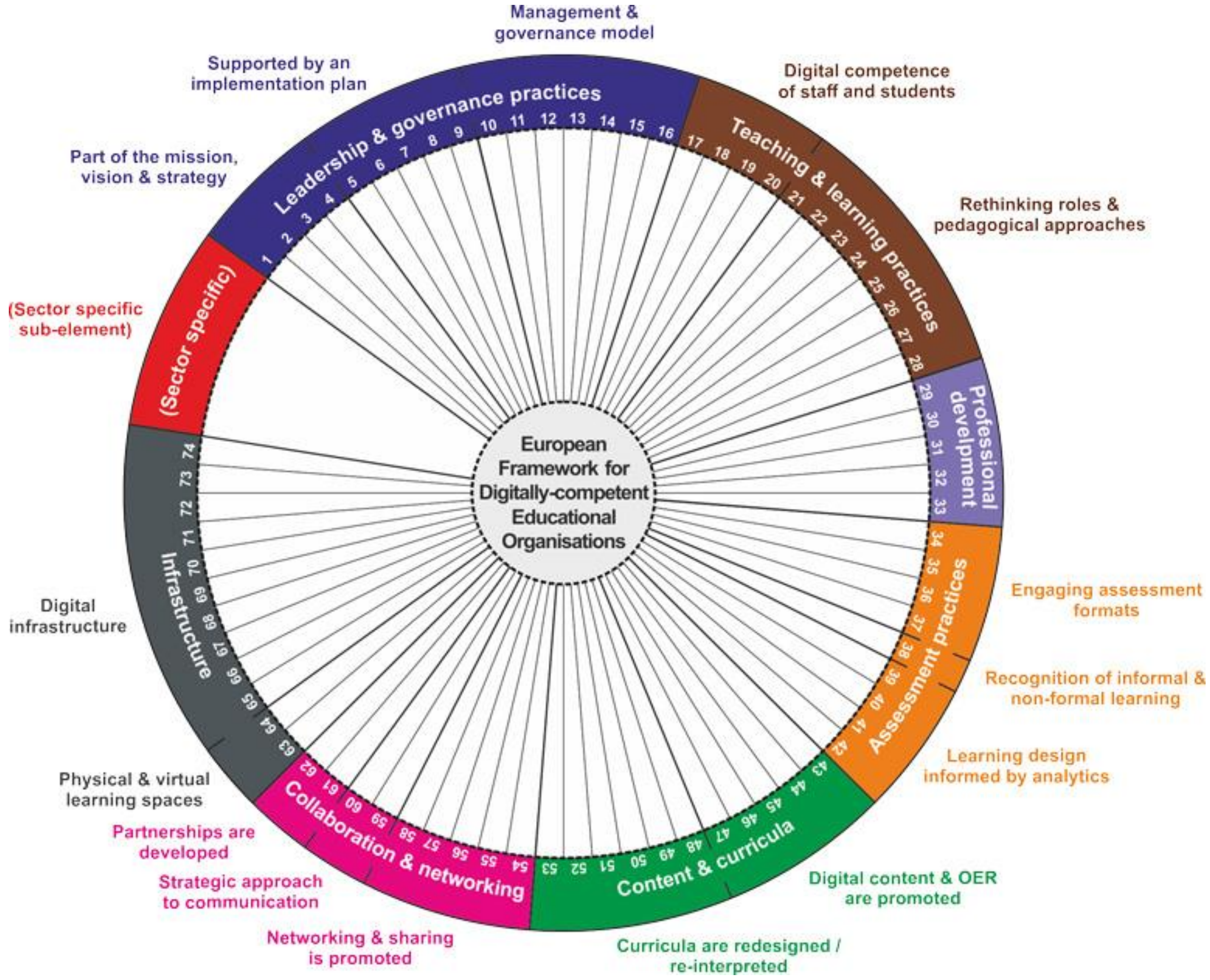


Fig. 3 - European Framework for Digitally-Competent Educational Organisations (DigCompOrg)[4]

[4] Image from "Joint Research Centre, Institute for Prospective Technological Studies, Devine, J., Punie, Y., Kampylis. Promoting effective digital-age learning – A European framework for digitally-competent educational organisations, Publications Office, 2015. https://dx.doi.org/10.2791/54070." © European Union, 2015.

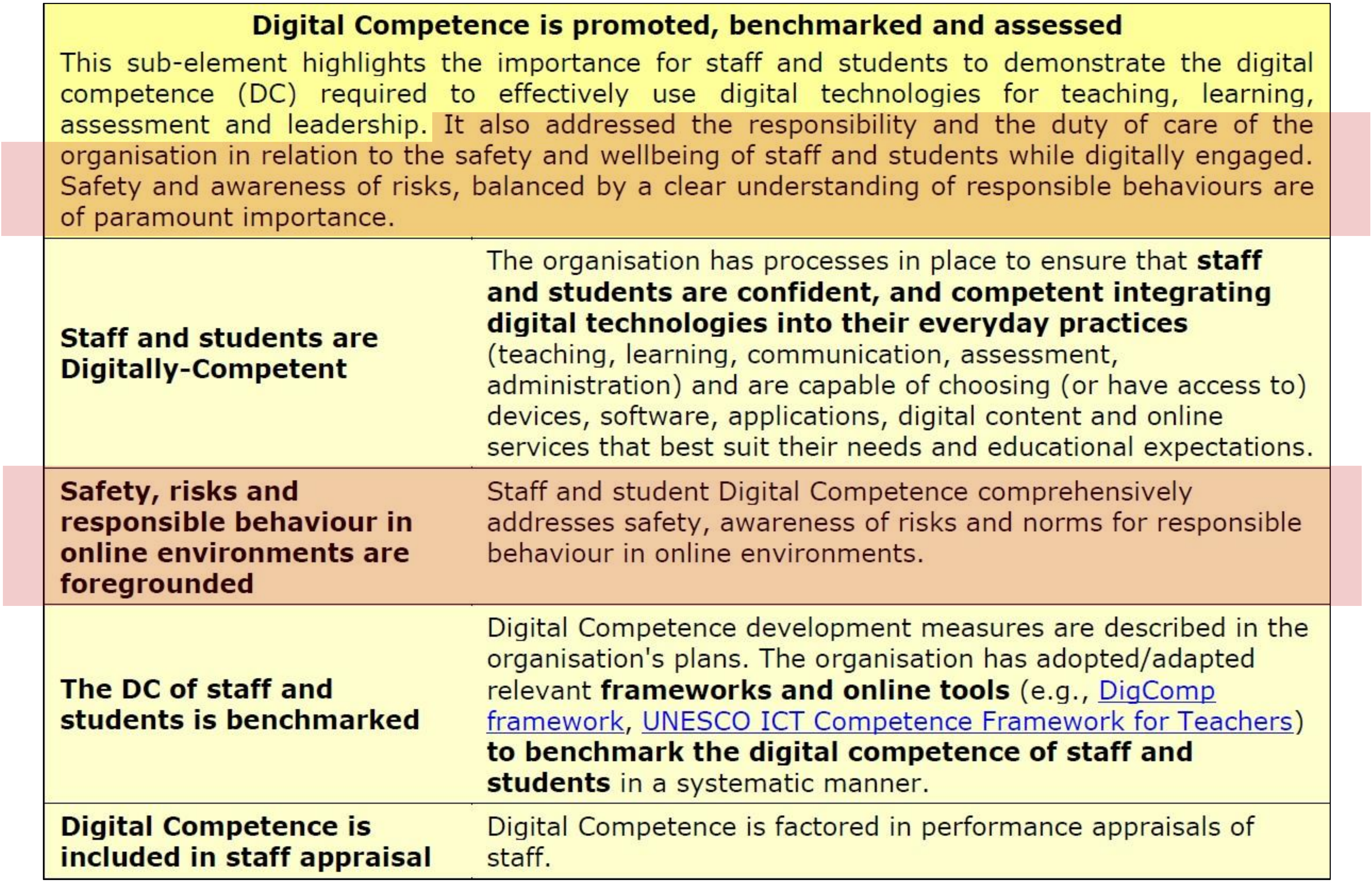
Organisational structure of DigCompOrg framework

• **Thematic element (and illustrative description)**	[macro competence area]
• **Sub-element (and illustrative description)**	[competence area]
• Descriptor (title-statement plus explanatory descriptor text)	[competence]

Coverage of cybersecurity domain in DigCompOrg framework

- **Teaching and Learning Practices**

- **Digital competence is promoted, benchmarked and assessed**



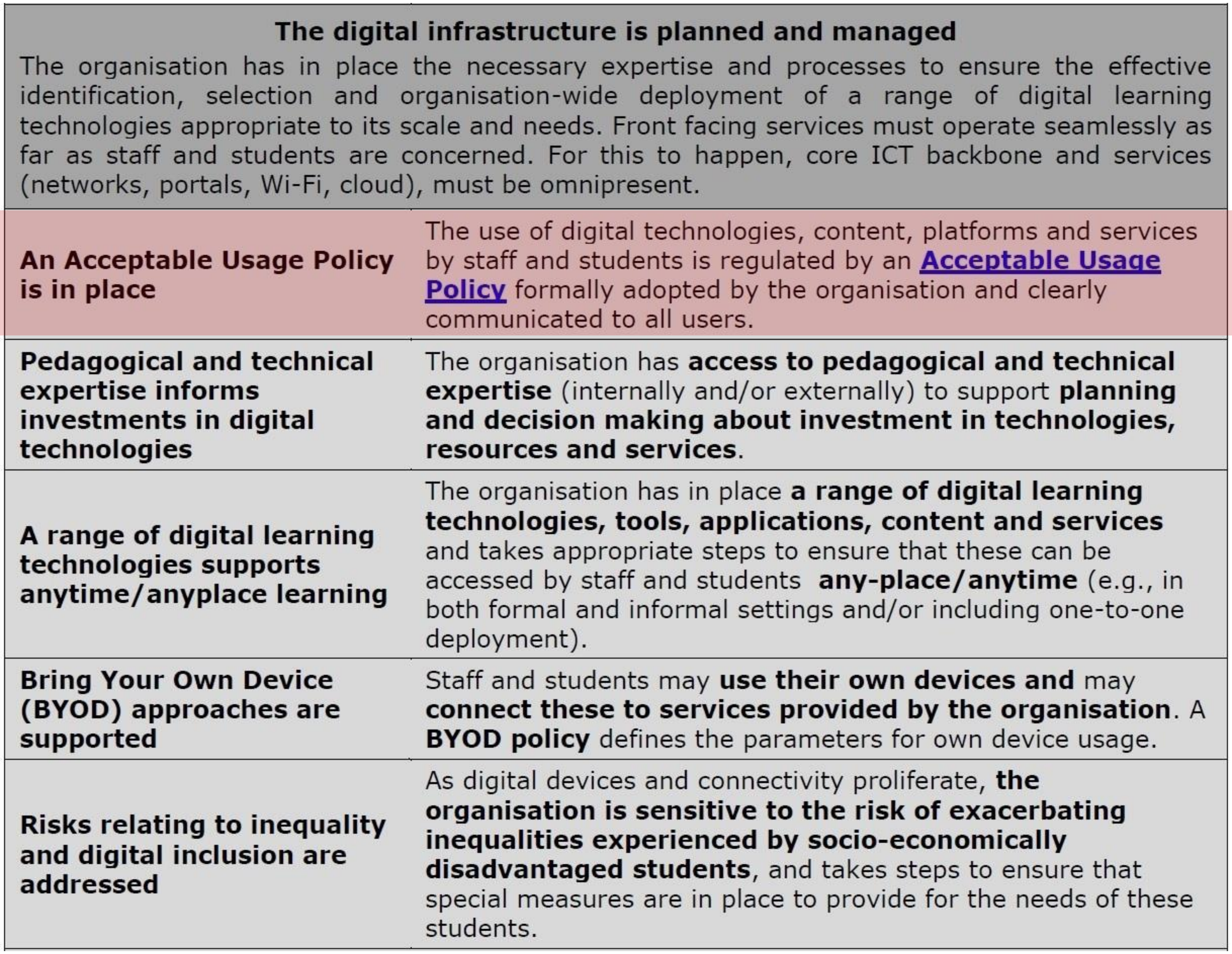
Digital Competence is promoted, benchmarked and assessed

This sub-element highlights the importance for staff and students to demonstrate the digital competence (DC) required to effectively use digital technologies for teaching, learning, assessment and leadership. It also addressed the responsibility and the duty of care of the organisation in relation to the safety and wellbeing of staff and students while digitally engaged. Safety and awareness of risks, balanced by a clear understanding of responsible behaviours are of paramount importance.

Staff and students are Digitally-Competent	The organisation has processes in place to ensure that **staff and students are confident, and competent integrating digital technologies into their everyday practices** (teaching, learning, communication, assessment, administration) and are capable of choosing (or have access to) devices, software, applications, digital content and online services that best suit their needs and educational expectations.
Safety, risks and responsible behaviour in online environments are foregrounded	Staff and student Digital Competence comprehensively addresses safety, awareness of risks and norms for responsible behaviour in online environments.
The DC of staff and students is benchmarked	Digital Competence development measures are described in the organisation's plans. The organisation has adopted/adapted relevant **frameworks and online tools** (e.g., DigComp framework, UNESCO ICT Competence Framework for Teachers) **to benchmark the digital competence of staff and students** in a systematic manner.
Digital Competence is included in staff appraisal	Digital Competence is factored in performance appraisals of staff.

- # Infrastructure

- ## The digital infrastructure is planned and managed

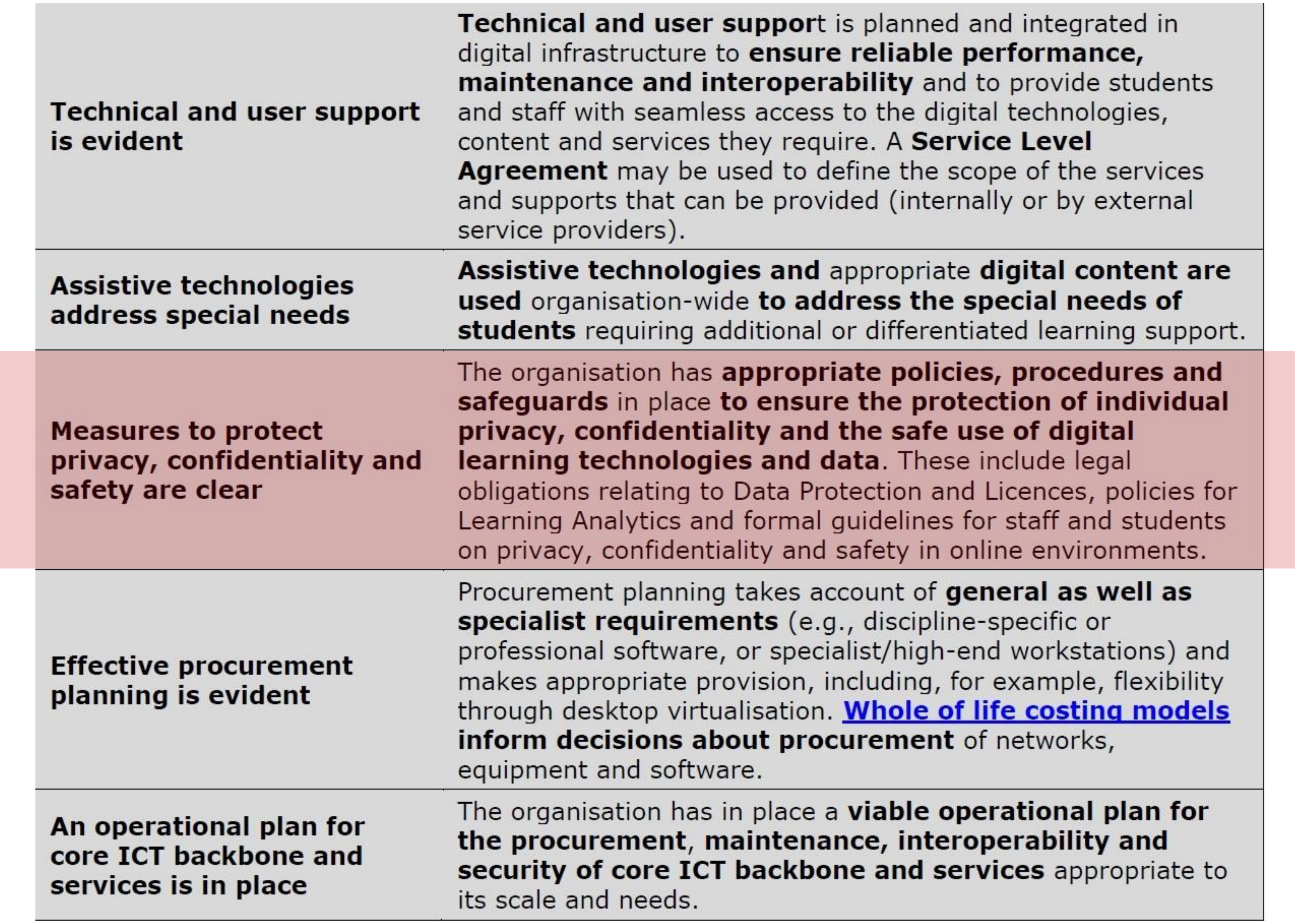


The digital infrastructure is planned and managed

The organisation has in place the necessary expertise and processes to ensure the effective identification, selection and organisation-wide deployment of a range of digital learning technologies appropriate to its scale and needs. Front facing services must operate seamlessly as far as staff and students are concerned. For this to happen, core ICT backbone and services (networks, portals, Wi-Fi, cloud), must be omnipresent.

An Acceptable Usage Policy is in place	The use of digital technologies, content, platforms and services by staff and students is regulated by an **Acceptable Usage Policy** formally adopted by the organisation and clearly communicated to all users.
Pedagogical and technical expertise informs investments in digital technologies	The organisation has **access to pedagogical and technical expertise** (internally and/or externally) to support **planning and decision making about investment in technologies, resources and services**.
A range of digital learning technologies supports anytime/anyplace learning	The organisation has in place **a range of digital learning technologies, tools, applications, content and services** and takes appropriate steps to ensure that these can be accessed by staff and students **any-place/anytime** (e.g., in both formal and informal settings and/or including one-to-one deployment).
Bring Your Own Device (BYOD) approaches are supported	Staff and students may **use their own devices and** may **connect these to services provided by the organisation**. A **BYOD policy** defines the parameters for own device usage.
Risks relating to inequality and digital inclusion are addressed	As digital devices and connectivity proliferate, **the organisation is sensitive to the risk of exacerbating inequalities experienced by socio-economically disadvantaged students**, and takes steps to ensure that special measures are in place to provide for the needs of these students.

[5]



Technical and user support is evident	**Technical and user suppor**t is planned and integrated in digital infrastructure to **ensure reliable performance, maintenance and interoperability** and to provide students and staff with seamless access to the digital technologies, content and services they require. A **Service Level Agreement** may be used to define the scope of the services and supports that can be provided (internally or by external service providers).
Assistive technologies address special needs	**Assistive technologies and** appropriate **digital content are used** organisation-wide **to address the special needs of students** requiring additional or differentiated learning support.
Measures to protect privacy, confidentiality and safety are clear	The organisation has **appropriate policies, procedures and safeguards** in place **to ensure the protection of individual privacy, confidentiality and the safe use of digital learning technologies and data**. These include legal obligations relating to Data Protection and Licences, policies for Learning Analytics and formal guidelines for staff and students on privacy, confidentiality and safety in online environments.
Effective procurement planning is evident	Procurement planning takes account of **general as well as specialist requirements** (e.g., discipline-specific or professional software, or specialist/high-end workstations) and makes appropriate provision, including, for example, flexibility through desktop virtualisation. **Whole of life costing models inform decisions about procurement** of networks, equipment and software.
An operational plan for core ICT backbone and services is in place	The organisation has in place a **viable operational plan for the procurement**, **maintenance, interoperability and security of core ICT backbone and services** appropriate to its scale and needs.

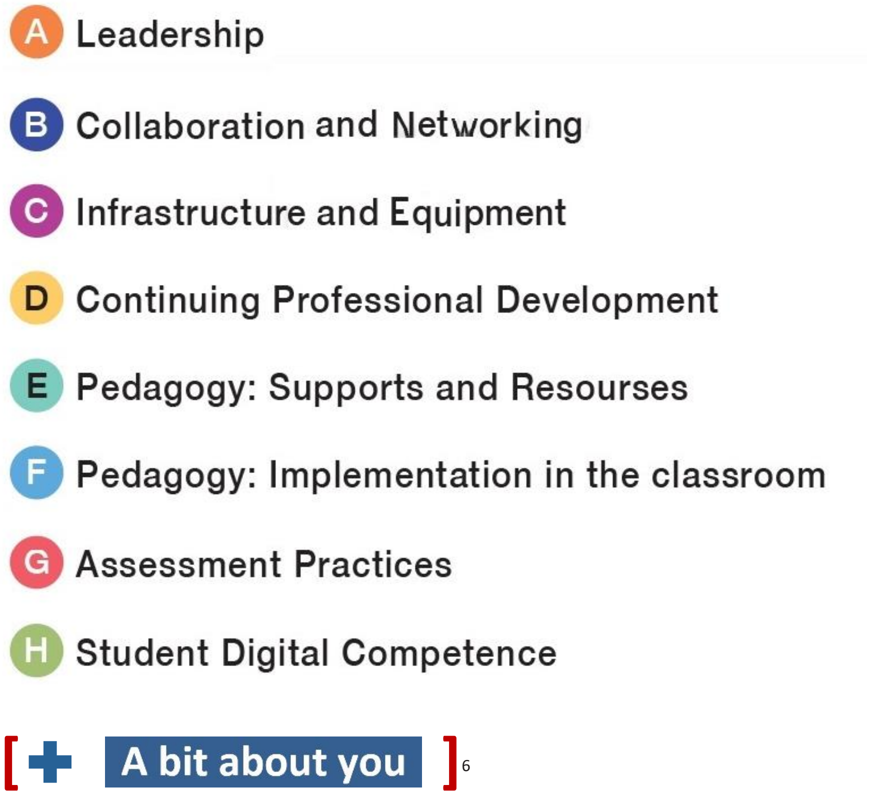
[5] Tables on this and preceding pages from "Joint Research Centre, Institute for Prospective Technological Studies, Devine, J., Punie, Y., Kampylis. Promoting effective digital-age learning – A European framework for digitally-competent educational organisations, Publications Office, 2015. https://dx.doi.org/10.2791/54070." © European Union, 2015: emphasis added

2.3 **[SELFIE] -** Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies

self-assessment tool	SELFIE (Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies)
versioning	v1 (2018) and subsequent rolling updates
description	*"SELFIE is a free self-assessment tool designed to help individual schools embed digital technologies into teaching, learning and assessment ... [and gain] a better understanding of how digital technologies are [being] used … [It involves] students, teachers and school leaders in a collective reflection on technology use [in their school] … It is anonymous and customisable: the school can select and add questions and statements to personalise their SELFIE questionnaires and, [on completion], receive a tailor-made, interactive report which provides both in-depth data and quick insights into strengths and weaknesses. SELFIE … [is] based on the EC's **Digital Competence Framework for Digitally Competent Educational Organisations (DigCompOrg**)"* [see previous entry in this document] SELFIE comprises a set of distinct online self-assessment surveys respectively addressing school leaders, teachers, and students (min. age = 8), at different levels of compulsory education: primary, lower secondary, upper secondary, upper secondary VET. Respondents are requested to consider the individual survey statements ("In our school…."), reflect on their experience of (or position on) each one within their school's learning community, and rate this on a 5-point scale from "strongly agree" to "strongly disagree" (plus a "non-applicable" option). Each SELFIE survey comprises a set of core items, i.e. those largely common to all education levels. But the school's SELFIE team can opt to include some optional items (selected by from a pre-defined set of optional indicators), and also create and add self-defined items that the team feels meet the school's own particular needs (a pre-set template is available for this purpose).
primary target	Learning communities in primary, secondary, and upper-secondary vocational (VET) schools, comprising School Leaders, Teachers, Students (8 y.o.+)
organisation & structure	Eight thematic competence areas grouping **49 core competence/capacity items** and **18 optional items** (total = 67 items), plus an additional section called ("*A bit about you*") for gathering basic profile information, plus personal views and experience (SELFIE survey responses are anonymous throughout). The "*A bit about you"* section contains **28 core items** and **4 optional items** (total = 32 items). So in 'factory-setting' mode, SELFIE proposes a maximum of **77 core items** and **22 optional items**. The core and optional items can be supplemented with self-defined items generated using a standard template form.
cybersecurity coverage	Two of the eight competence areas ("Student Digital Competence" and "Infrastructure and Equipment") include core competence items related to cybersecurity: in the former case "Safe Behaviour" and Responsible Behaviour", and in the latter "Data protection ".

self-assessment tool (cont.)	SELFIE (Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies)
EC platform	https://education.ec.europa.eu/selfie
gateway access	https://schools-go-digital.jrc.ec.europa.eu/school/registry
main EC publications	• European Commission (2021). SELFIE Guide for School Coordinators • European Commission (2022) Discover the Digital Potential of Your School – SELFIE Questionnaires (EN) • Joint Research Centre, Institute for Prospective Technological Studies, Devine, J., Punie, Y., Kampylis. (2015) Promoting effective digital-age learning – A European framework for digitally-competent educational organisations, Publications Office, 2015, https://data.europa.eu/doi/10.2791/54070 [© European Union, 2015 (*“Reproduction is authorised provided the source is acknowledged.”*)]

Domain scope of SELFIE tool



A Leadership

B Collaboration and Networking

C Infrastructure and Equipment

D Continuing Professional Development

E Pedagogy: Supports and Resourses

F Pedagogy: Implementation in the classroom

G Assessment Practices

H Student Digital Competence

[+ A bit about you][6]

[6] List from European Commission (2021) SELFIE Guide for School Coordinators, with author's additions

Organisational structure of SELFIE

- **Competence area (and brief description)**

- **Competence item (ID code + title)**

- *Competence statement* [e.g. "In our school, ……" statement reifying the competence]

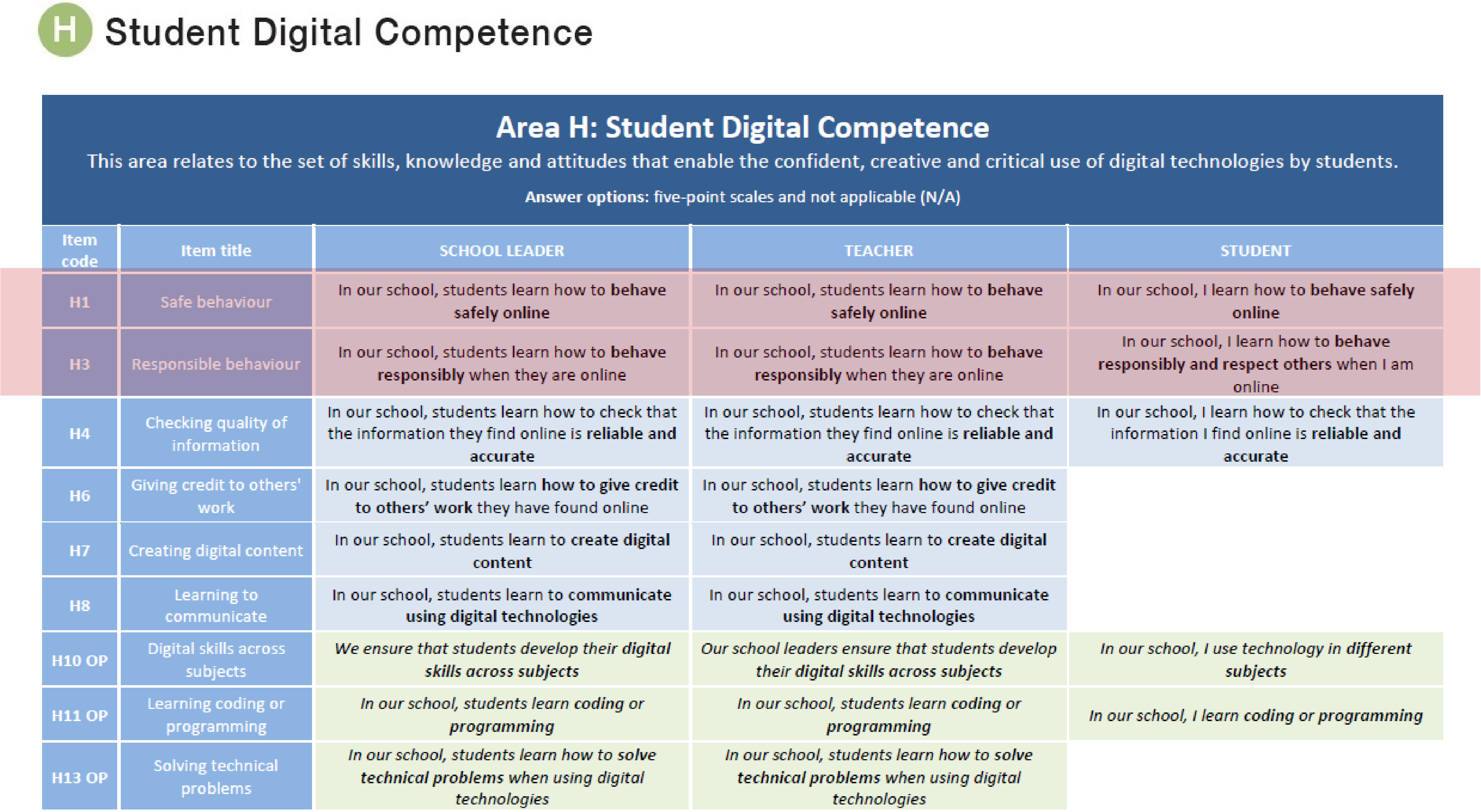
- SELFIE user profile [SCHOOL LEADER, TEACHER, STUDENT – for target-specific questionnaires]

  [Participants respond to item statements on a 5-point scale, from "strongly agree" to "strongly disagree"]

- *Additional individual information ("A bit about you")*

  [Participants respond to "A bit about you" item statements mostly from pull-down menus presenting predefined response options]

Coverage of cybersecurity domain in SELFIE



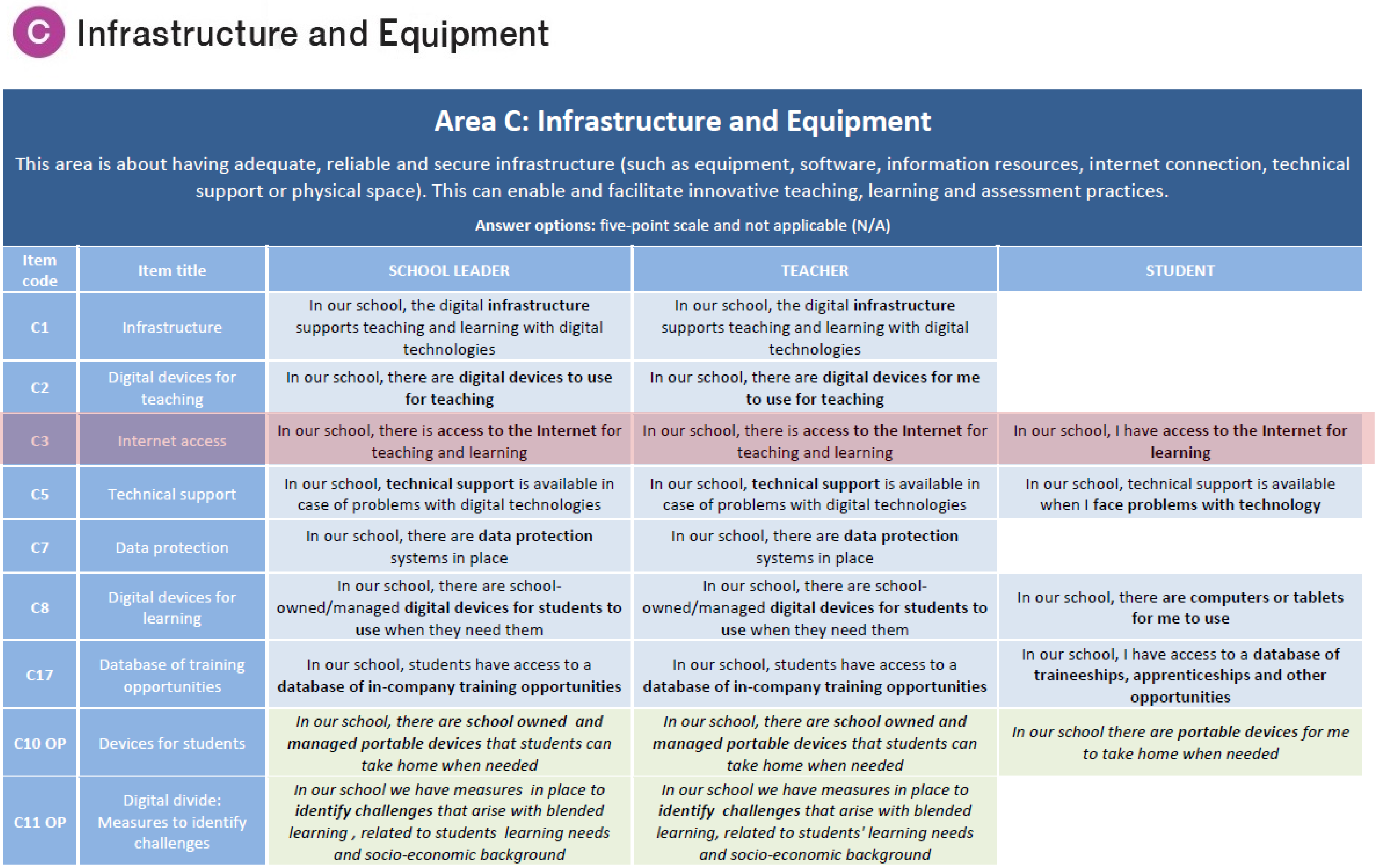
H Student Digital Competence

Area H: Student Digital Competence

This area relates to the set of skills, knowledge and attitudes that enable the confident, creative and critical use of digital technologies by students.

Answer options: five-point scales and not applicable (N/A)

Item code	Item title	SCHOOL LEADER	TEACHER	STUDENT
H1	Safe behaviour	In our school, students learn how to **behave safely online**	In our school, students learn how to **behave safely online**	In our school, I learn how to **behave safely online**
H3	Responsible behaviour	In our school, students learn how to **behave responsibly** when they are online	In our school, students learn how to **behave responsibly** when they are online	In our school, I learn how to **behave responsibly and respect others** when I am online
H4	Checking quality of information	In our school, students learn how to check that the information they find online is **reliable and accurate**	In our school, students learn how to check that the information they find online is **reliable and accurate**	In our school, I learn how to check that the information I find online is **reliable and accurate**
H6	Giving credit to others' work	In our school, students learn **how to give credit to others' work** they have found online	In our school, students learn **how to give credit to others' work** they have found online	
H7	Creating digital content	In our school, students learn to **create digital content**	In our school, students learn to **create digital content**	
H8	Learning to communicate	In our school, students learn to **communicate using digital technologies**	In our school, students learn to **communicate using digital technologies**	
H10 OP	Digital skills across subjects	*We ensure that students develop their digital **skills across subjects***	*Our school leaders ensure that students develop their **digital skills across subjects***	*In our school, I use technology in **different subjects***
H11 OP	Learning coding or programming	*In our school, students learn **coding or programming***	*In our school, students learn **coding or programming***	*In our school, I learn **coding or programming***
H13 OP	Solving technical problems	*In our school, students learn how to solve **technical problems** when using digital technologies*	*In our school, students learn how to solve **technical problems** when using digital technologies*	



C Infrastructure and Equipment

Area C: Infrastructure and Equipment

This area is about having adequate, reliable and secure infrastructure (such as equipment, software, information resources, internet connection, technical support or physical space). This can enable and facilitate innovative teaching, learning and assessment practices.

Answer options: five-point scale and not applicable (N/A)

Item code	Item title	SCHOOL LEADER	TEACHER	STUDENT
C1	Infrastructure	In our school, the digital **infrastructure** supports teaching and learning with digital technologies	In our school, the digital **infrastructure** supports teaching and learning with digital technologies	
C2	Digital devices for teaching	In our school, there are **digital devices to use for teaching**	In our school, there are **digital devices for me to use for teaching**	
C3	Internet access	In our school, there is **access to the Internet** for teaching and learning	In our school, there is **access to the Internet** for teaching and learning	In our school, I have **access to the Internet** for **learning**
C5	Technical support	In our school, **technical support** is available in case of problems with digital technologies	In our school, **technical support** is available in case of problems with digital technologies	In our school, technical support is available when I **face problems with technology**
C7	Data protection	In our school, there are **data protection** systems in place	In our school, there are **data protection** systems in place	
C8	Digital devices for learning	In our school, there are school-owned/managed **digital devices for students to use** when they need them	In our school, there are school-owned/managed **digital devices for students to use** when they need them	In our school, there **are computers or tablets for me to use**
C17	Database of training opportunities	In our school, students have access to a **database of in-company training opportunities**	In our school, students have access to a **database of in-company training opportunities**	In our school, I have access to a **database of traineeships, apprenticeships and other opportunities**
C10 OP	Devices for students	*In our school, there are school owned and managed portable devices that students can take home when needed*	*In our school, there are school owned and managed portable devices that students can take home when needed*	*In our school there are portable devices for me to take home when needed*
C11 OP	Digital divide: Measures to identify challenges	*In our school we have measures in place to identify challenges that arise with blended learning , related to students learning needs and socio-economic background*	*In our school we have measures in place to identify challenges that arise with blended learning, related to students' learning needs and socio-economic background*	

[7]

[7] Image on this and preceding page from European Commission (2022) Discover the Digital Potential of Your School – SELFIE Questionnaires (EN): emphasis added.

2.4. **[DigCompEdu]** - European Framework for the Digital Competence of Educators

Framework	The European Framework for the Digital Competence of Educators (DigCompEdu)
Versioning	DigCompEdu (2017)
Description	DigCompEdu is the EC's digital competency framework for educators. It underpins the digital education self-assessment tool SELFIEforTeachers (see next entry).
Primary target	Educators at all levels of education, from early childhood to higher and adult education, including general and vocational education and training, special needs education, and non-formal learning contexts
Organisation & structure	Three profile-based macro areas grouping six competence areas that cover 32 competence items. Each competence has a general descriptor and a list of activities typically associated with that competence. The competence framework is coupled with a "progression model", a six-level scale of proficiency in each of the 32 competences. Each proficiency level has one or more proficiency statements ("I foster…", "I develop …", etc.)
Cybersecurity coverage	Two of the six competence areas, *Facilitating Learners' Digital Competence* and *Digital Resources*, include competence items related to cybersecurity: in the former case these competence items are *Responsible use* and (only nominatively) Communication, while cybersecurity is touched on in *Managing, Protecting, Sharing*.
EC Platform	https://joint-research-centre.ec.europa.eu/digcompedu_en
Main EC publications	• Redecker, C. **European Framework for the Digital Competence of Educators: DigCompEdu**. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466 [© European Union, 2017 "Reuse is authorised provided the source is acknowledged"] • Economou, A., SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

Domain scope of DigCompEdu

[The DigCompEdu framework comprises 3 profile-based macro areas, 6 digital competence areas, and 32 competences.]

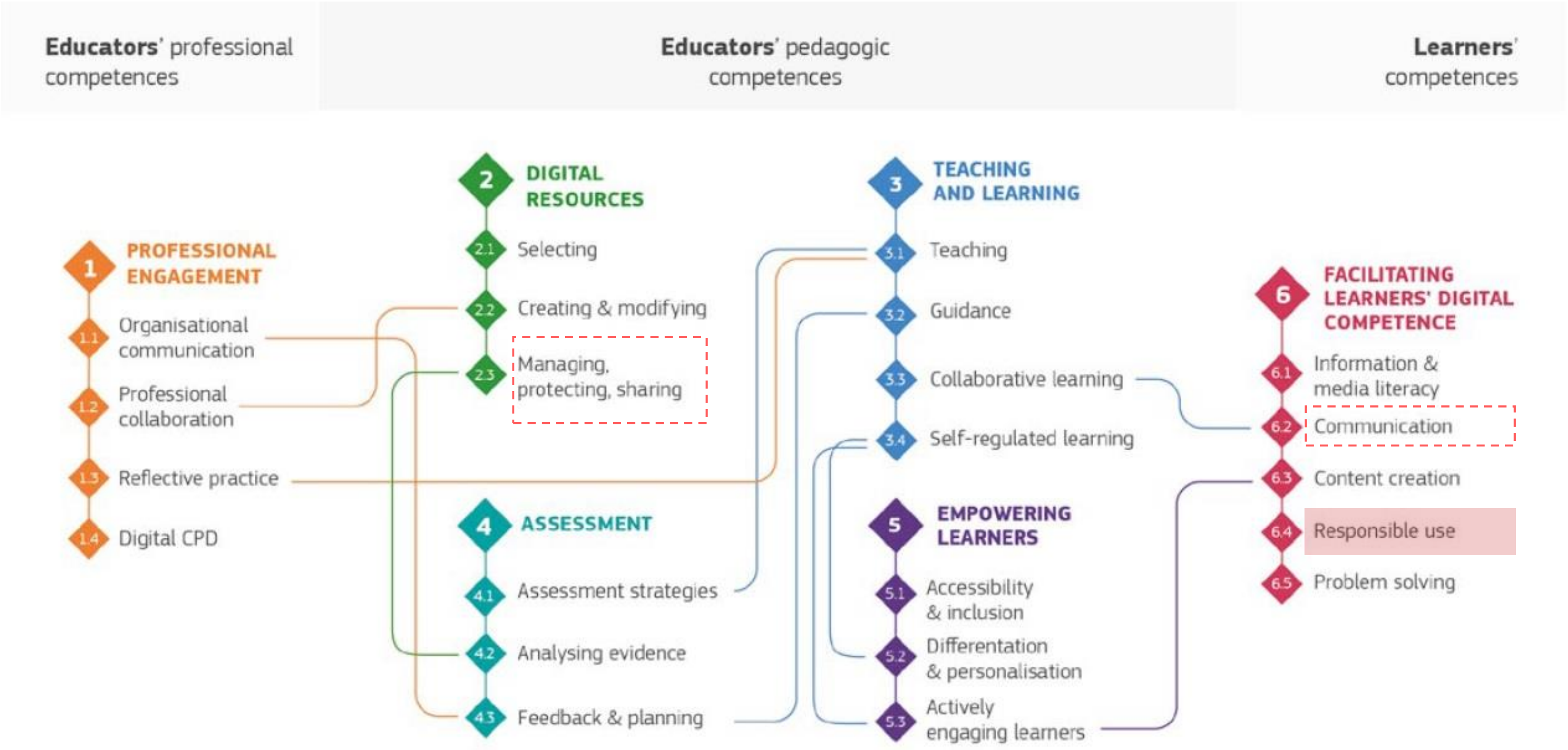

Educators' professional competences
Educators' pedagogic competences
Learners' competences
1 PROFESSIONAL ENGAGEMENT
1.1 Organisational communication
1.2 Professional collaboration
1.3 Reflective practice
1.4 Digital CPD
2 DIGITAL RESOURCES
2.1 Selecting
2.2 Creating & modifying
2.3 Managing, protecting, sharing
3 TEACHING AND LEARNING
3.1 Teaching
3.2 Guidance
3.3 Collaborative learning
3.4 Self-regulated learning
4 ASSESSMENT
4.1 Assessment strategies
4.2 Analysing evidence
4.3 Feedback & planning
5 EMPOWERING LEARNERS
5.1 Accessibility & inclusion
5.2 Differentiation & personalisation
5.3 Actively engaging learners
6 FACILITATING LEARNERS' DIGITAL COMPETENCE
6.1 Information & media literacy
6.2 Communication
6.3 Content creation
6.4 Responsible use
6.5 Problem solving

Fig. 4 - DigCompEdu's competence framework with cybersecurity-related competences highlighted[8]

[8] Image from Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466. © European Union, 2017: emphasis added

[The DigCompEdu framework incorporates a conceptual “progression model” of graduated proficiency.]

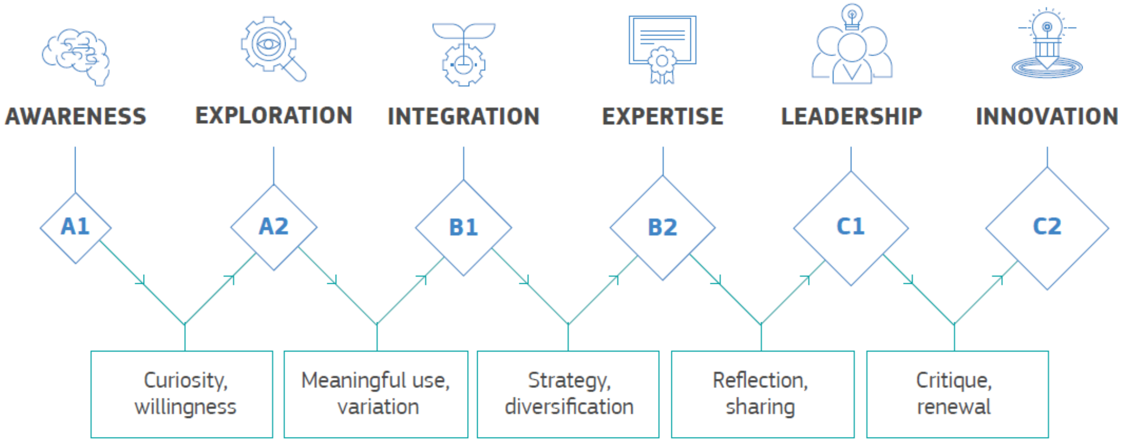
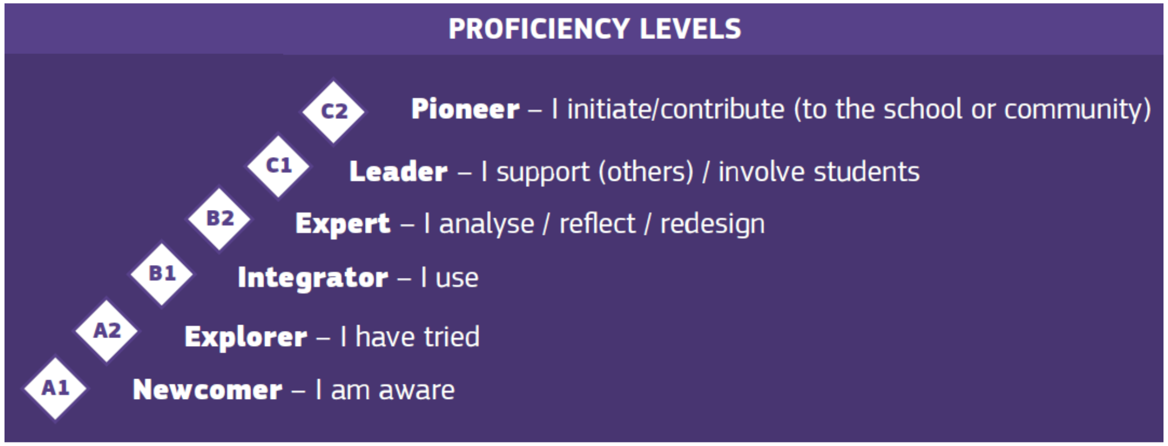


Fig. 5 - DigCompEdu Progression Model[9]

[On the basis of this model, each competence is reified through a set of exemplary actions that are ranked in eight proficiency levels, each labelled as a profile ranging from ‘newcomer’ to ‘pioneer’.]

[9] Image from Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466. © European Union, 2017.



PROFICIENCY LEVELS

C2 **Pioneer** – I initiate/contribute (to the school or community)

C1 **Leader** – I support (others) / involve students

B2 **Expert** – I analyse / reflect / redesign

B1 **Integrator** – I use

A2 **Explorer** – I have tried

A1 **Newcomer** – I am aware

Fig. 6 - DigCompEdu graded proficiency levels[10]

Organisational structure of DigCompEdu

- **COMPETENCE AREA**
- **COMPETENCE**
- **Activities** [List of activities associated with the competence]
- Competence progression levels [Proficiency levels (1-6) for each competence, inc. general description]
- Competence *proficiency statement/s* [Set of six “I foster ….; I develop….” statements reifying each competence at each of the six progression levels].

[10] Image from Economou, A., SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

Coverage of cybersecurity domain in DigCompEdu

6. FACILITATING LEARNERS' DIGITAL COMPETENCE

6.4. RESPONSIBLE USE

To protect devices and digital content, and to understand risks and threats in digital environments.
To know about safety and security measures and to have a due regard to reliability and privacy.

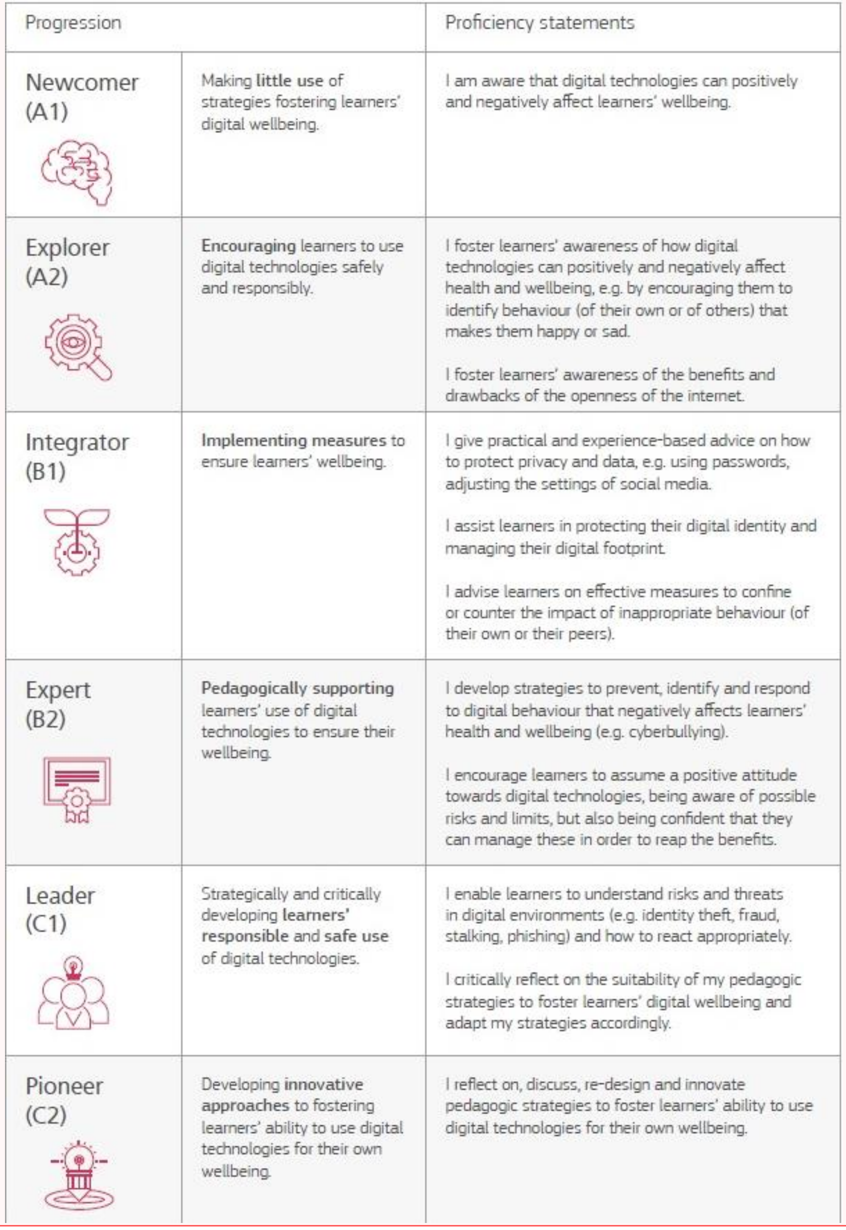
Activities

Activity: enable learners to….

- protect devices and digital content, and to understand risks and threats in digital environments.
- understand safety and security measures.
- protect personal data and privacy in digital environments.
- understand how to use and share personal information while being able to protect oneself and others from damages.
- understand that digital services use a "Privacy policy" on how personal data is used.
- avoid health risks and threats to physical and psychological well-being while using digital technologies.
- protect oneself and others from possible dangers in digital environments (e.g. cyberbullying).
- be aware of digital technologies for social wellbeing and social inclusion.
- be aware of the environmental impact of digital technologies and their use.

Activity: monitor student behaviour in digital environments in order to safeguard their wellbeing.

Activity: react immediately and effectively when learners' wellbeing is threatened in digital environments (e.g. cyberbullying).



Progression		Proficiency statements
Newcomer (A1)	Making **little use** of strategies fostering learners' digital wellbeing.	I am aware that digital technologies can positively and negatively affect learners' wellbeing.
Explorer (A2)	**Encouraging** learners to use digital technologies safely and responsibly.	I foster learners' awareness of how digital technologies can positively and negatively affect health and wellbeing, e.g. by encouraging them to identify behaviour (of their own or of others) that makes them happy or sad. I foster learners' awareness of the benefits and drawbacks of the openness of the internet.
Integrator (B1)	**Implementing measures** to ensure learners' wellbeing.	I give practical and experience-based advice on how to protect privacy and data, e.g. using passwords, adjusting the settings of social media. I assist learners in protecting their digital identity and managing their digital footprint. I advise learners on effective measures to confine or counter the impact of inappropriate behaviour (of their own or their peers).
Expert (B2)	**Pedagogically supporting** learners' use of digital technologies to ensure their wellbeing.	I develop strategies to prevent, identify and respond to digital behaviour that negatively affects learners' health and wellbeing (e.g. cyberbullying). I encourage learners to assume a positive attitude towards digital technologies, being aware of possible risks and limits, but also being confident that they can manage these in order to reap the benefits.
Leader (C1)	Strategically and critically developing **learners' responsible** and **safe use** of digital technologies.	I enable learners to understand risks and threats in digital environments (e.g. identity theft, fraud, stalking, phishing) and how to react appropriately. I critically reflect on the suitability of my pedagogic strategies to foster learners' digital wellbeing and adapt my strategies accordingly.
Pioneer (C2)	Developing **innovative approaches** to fostering learners' ability to use digital technologies for their own wellbeing.	I reflect on, discuss, re-design and innovate pedagogic strategies to foster learners' ability to use digital technologies for their own wellbeing.

6.2 Digital communication & collaboration

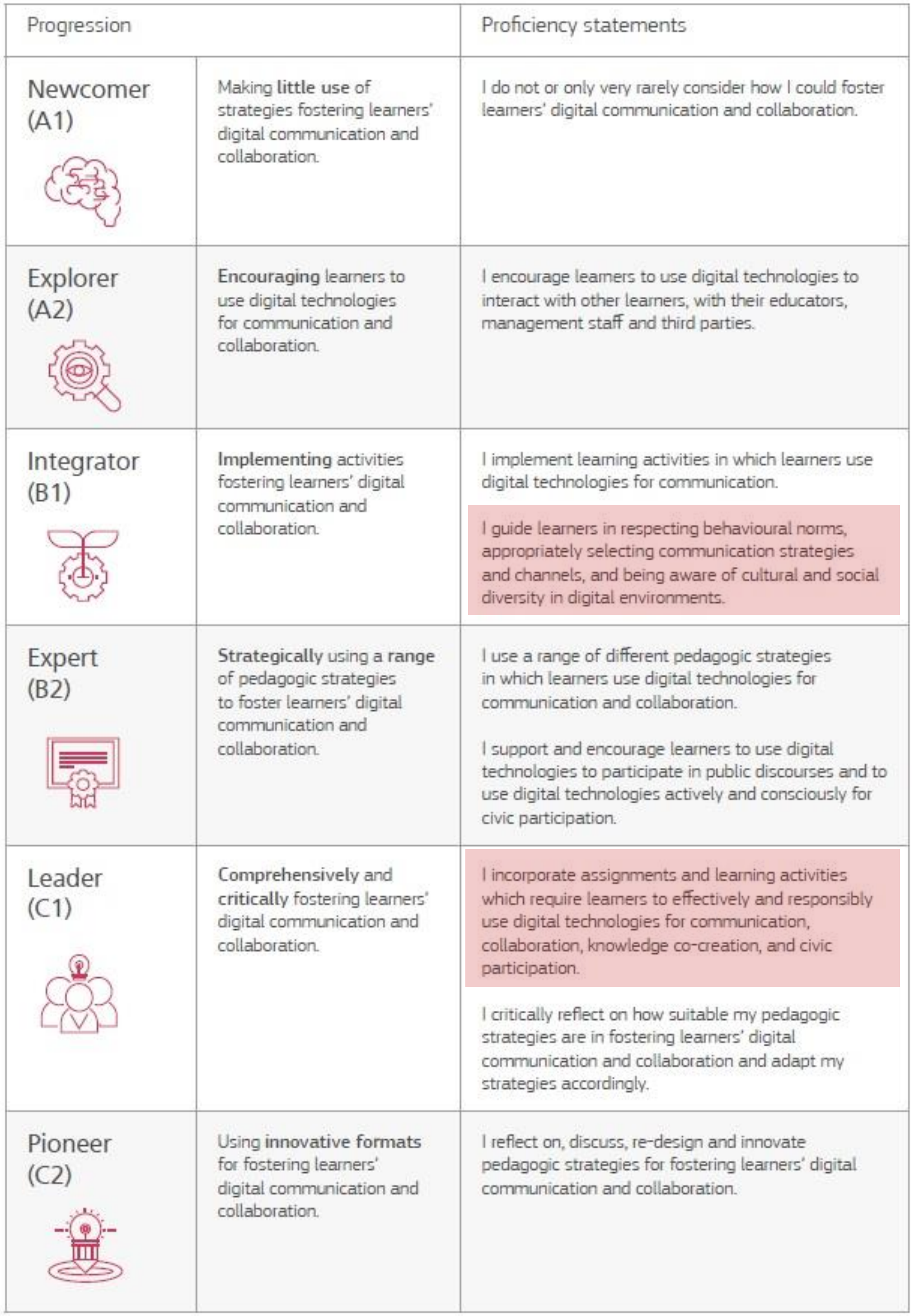
To incorporate learning activities, assignments and assessments which require learners to effectively and responsibly use digital technologies for communication, collaboration and civic participation.

Activities

Activity: To be aware of behavioural norms and know-how while using digital technologies and interacting in digital environments.

Activity: To create and manage one or multiple digital identities.

Activity: To protect one's own reputation.



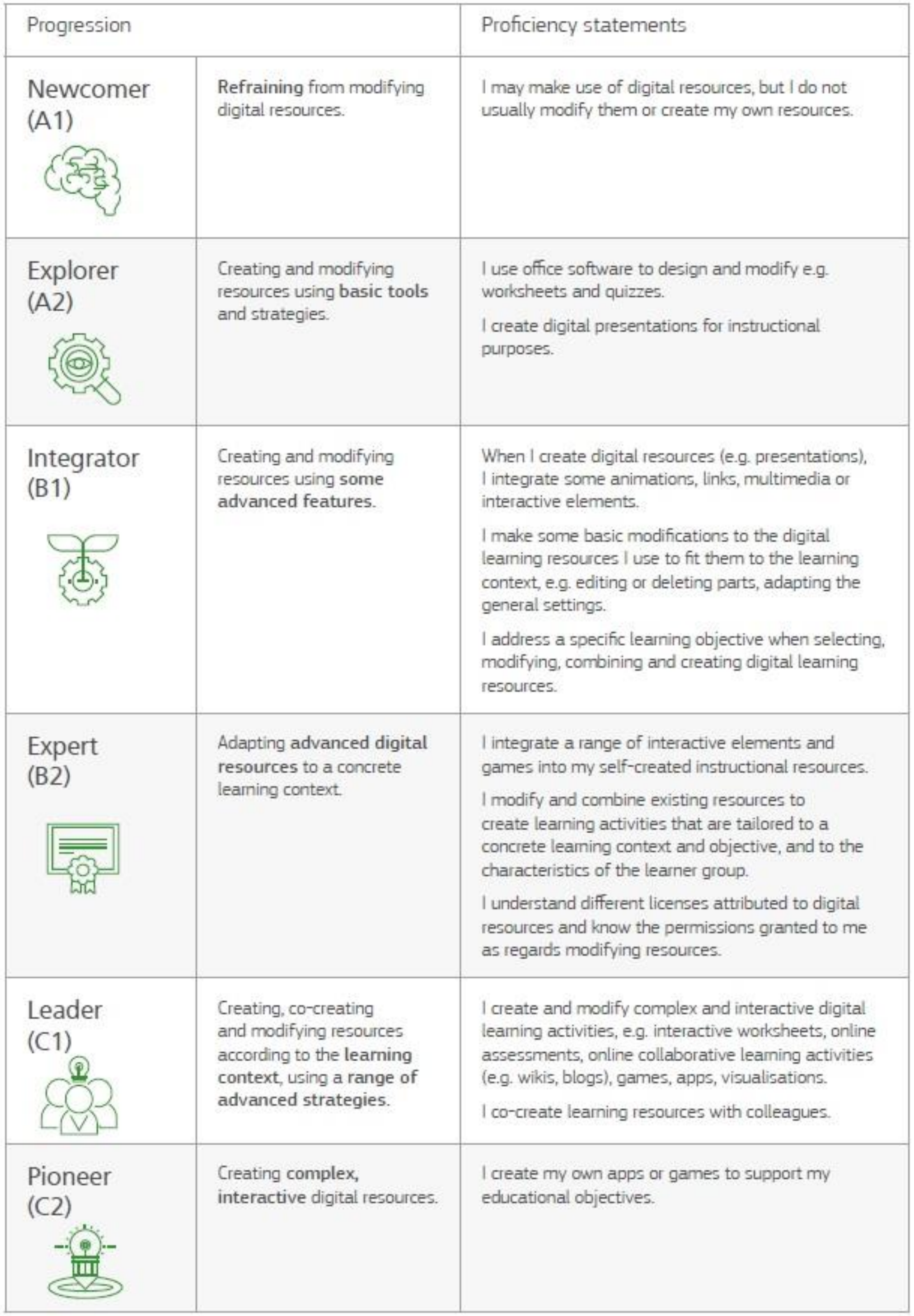
Progression		Proficiency statements
Newcomer (A1)	Making **little use** of strategies fostering learners' digital communication and collaboration.	I do not or only very rarely consider how I could foster learners' digital communication and collaboration.
Explorer (A2)	**Encouraging** learners to use digital technologies for communication and collaboration.	I encourage learners to use digital technologies to interact with other learners, with their educators, management staff and third parties.
Integrator (B1)	**Implementing** activities fostering learners' digital communication and collaboration.	I implement learning activities in which learners use digital technologies for communication. I guide learners in respecting behavioural norms, appropriately selecting communication strategies and channels, and being aware of cultural and social diversity in digital environments.
Expert (B2)	**Strategically** using a **range** of pedagogic strategies to foster learners' digital communication and collaboration.	I use a range of different pedagogic strategies in which learners use digital technologies for communication and collaboration. I support and encourage learners to use digital technologies to participate in public discourses and to use digital technologies actively and consciously for civic participation.
Leader (C1)	**Comprehensively** and **critically** fostering learners' digital communication and collaboration.	I incorporate assignments and learning activities which require learners to effectively and responsibly use digital technologies for communication, collaboration, knowledge co-creation, and civic participation. I critically reflect on how suitable my pedagogic strategies are in fostering learners' digital communication and collaboration and adapt my strategies accordingly.
Pioneer (C2)	Using **innovative formats** for fostering learners' digital communication and collaboration.	I reflect on, discuss, re-design and innovate pedagogic strategies for fostering learners' digital communication and collaboration.

2. DIGITAL RESOURCES

2.3. Managing, protecting and sharing digital resources

To organise digital content and make it available to learners, parents and other educators. To effectively protect sensitive digital content. To respect and correctly apply privacy and copyright rules. To understand the use and creation of open licenses and open educational resources, including their proper attribution.

[Note: no further mention of privacy issues is made in the related competence activities, progression levels or proficiency statements]



Progression		Proficiency statements
Newcomer (A1)	**Refraining** from modifying digital resources.	I may make use of digital resources, but I do not usually modify them or create my own resources.
Explorer (A2)	Creating and modifying resources using **basic tools** and strategies.	I use office software to design and modify e.g. worksheets and quizzes. I create digital presentations for instructional purposes.
Integrator (B1)	Creating and modifying resources using **some advanced features.**	When I create digital resources (e.g. presentations), I integrate some animations, links, multimedia or interactive elements. I make some basic modifications to the digital learning resources I use to fit them to the learning context, e.g. editing or deleting parts, adapting the general settings. I address a specific learning objective when selecting, modifying, combining and creating digital learning resources.
Expert (B2)	Adapting **advanced digital resources** to a concrete learning context.	I integrate a range of interactive elements and games into my self-created instructional resources. I modify and combine existing resources to create learning activities that are tailored to a concrete learning context and objective, and to the characteristics of the learner group. I understand different licenses attributed to digital resources and know the permissions granted to me as regards modifying resources.
Leader (C1)	Creating, co-creating and modifying resources according to the **learning context, using a range of advanced strategies.**	I create and modify complex and interactive digital learning activities, e.g. interactive worksheets, online assessments, online collaborative learning activities (e.g. wikis, blogs), games, apps, visualisations. I co-create learning resources with colleagues.
Pioneer (C2)	Creating **complex, interactive** digital resources.	I create my own apps or games to support my educational objectives.

Footnote: tables on this and preceeding two pages from Economou, A., SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699: emphasis added

2.5. [SELFIEforTEACHERS]

self-assessment tool	SELFIEforTEACHERS (based on The European Framework for the Digital Competence of Educators - DigCompEdu)
versioning	v1 2021; updated 2022
description	SELFIEforTEACHERS is a tool for primary and secondary school teachers that allows them to self-assess their digital competence, individually or as a cohort. SELFIEforTEACHERS uses self-reflection to support the process of professional development and encourages teachers to plan their own learning according to the results. The tool is based on DigCompEdu (see previous entry)
primary target	Teachers in primary and secondary schools
organisation & structure	Six competence areas grouping 32 competence items. Each competence area and individual competence item has an illustrative descriptor. This structure is coupled with a "progression model", a six-level scale of proficiency applied to all 32 competences. This permits each competence to be exemplified at progressive levels via a set of six competence statements ("I foster…", "I develop …", etc.) that reify the competence at the given proficiency level. The SELFIEforTEACHERS respondent selects the statement they identify most closely with.
cybersecurity coverage	Two of the six competence areas, *Facilitating Learners' Digital Competence* and *Digital Resources*, include competence items related to cybersecurity; these are *Responsible use* and *Managing, Protecting, Sharing,* respectively.
EC platform	https://joint-research-centre.ec.europa.eu/digcompedu_en
gateway access	https://educators-go-digital.jrc.ec.europa.eu/
main EC publication	Economou, A., SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

Domain scope of SELFIEforTeachers

The ***SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS*** (Economou, 2023) states***:**

> *"To develop SELFIEforTEACHERS, we used the European Digital Competence of Educators (**DigCompEdu**) as a benchmark for teachers' digital competence. We analysed the **specific competences as described in the DigCompEdu**, also taking into consideration **new and emerging pedagogical needs and approaches**. We then designed a number of **self-reflection items**, which included **examples** to help teachers understand how that particular competence can be applied in practice."*

Organisational structure of SELFIEforTeachers

The ***SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS*** (Economou, 2023)***** states**:**

> *SELFIEforTEACHERS involves two design and development aspects: (a) the **content**, which includes the **reflection items**, **examples**, **help text** explaining the terms used, and **proficiency level-based feedback** with **suggestions on how to level up**; and (b) the online platform to host the tool, which includes the user interface and functionalities.*

***emphasis** added

- **COMPETENCE AREA (and illustrative description)**

- **COMPETENCE (competence title & one-line descriptor)**

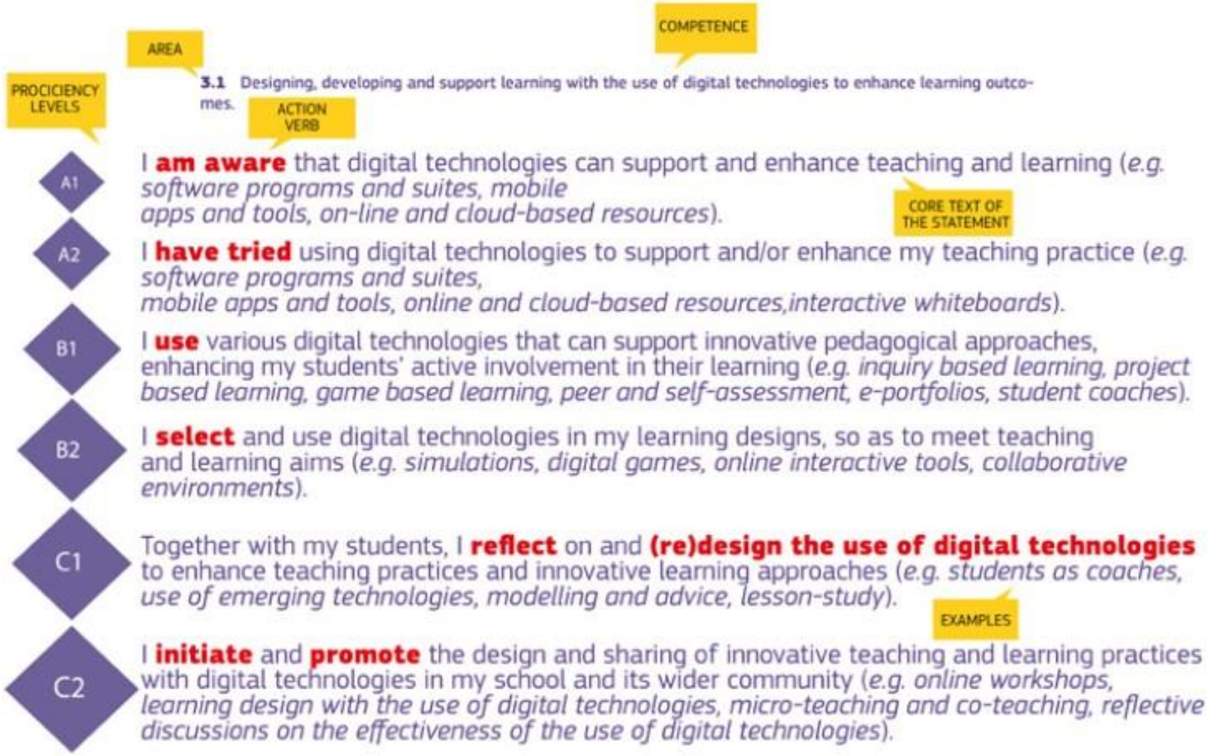
- **Competence progression levels**

[A1 – A2 – B1 – B2 – C1 – C2]

- Competence/*item statements*

[Statements (“I foster…”, “I develop …”, etc.)
reifying each competence at the 8 progression levels
and presented to the respondent for selection]

[Participants respond by selecting which competence proficiency statement mostly closely matches their own level]



3.1 Designing, developing and support learning with the use of digital technologies to enhance learning outcomes.

A1 I **am aware** that digital technologies can support and enhance teaching and learning (*e.g. software programs and suites, mobile apps and tools, on-line and cloud-based resources*).

A2 I **have tried** using digital technologies to support and/or enhance my teaching practice (*e.g. software programs and suites, mobile apps and tools, online and cloud-based resources,interactive whiteboards*).

B1 I **use** various digital technologies that can support innovative pedagogical approaches, enhancing my students' active involvement in their learning (*e.g. inquiry based learning, project based learning, game based learning, peer and self-assessment, e-portfolios, student coaches*).

B2 I **select** and use digital technologies in my learning designs, so as to meet teaching and learning aims (*e.g. simulations, digital games, online interactive tools, collaborative environments*).

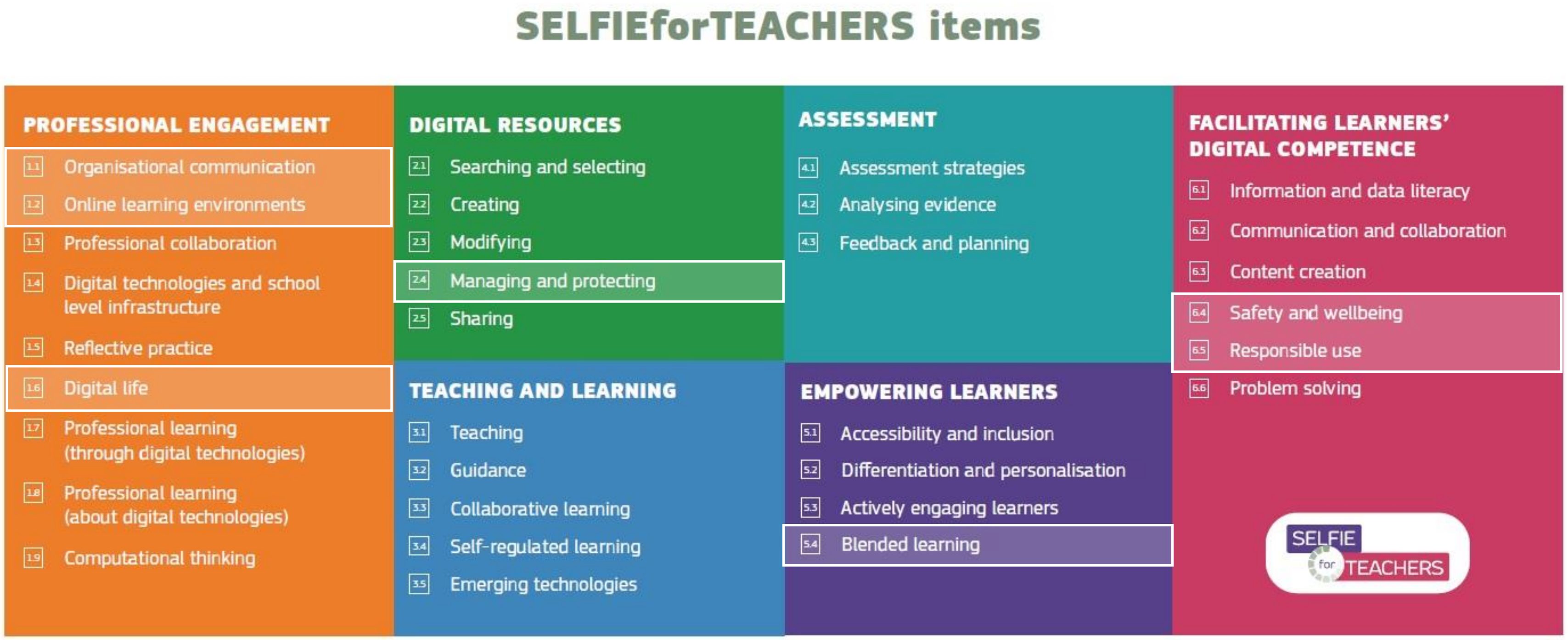
C1 Together with my students, I **reflect** on and **(re)design the use of digital technologies** to enhance teaching practices and innovative learning approaches (*e.g. students as coaches, use of emerging technologies, modelling and advice, lesson-study*).

C2 I **initiate** and **promote** the design and sharing of innovative teaching and learning practices with digital technologies in my school and its wider community (*e.g. online workshops, learning design with the use of digital technologies, micro-teaching and co-teaching, reflective discussions on the effectiveness of the use of digital technologies*).

Fig. 6 - SELFIEforTEACHERS structure of items (an example)[11]

[11] Figure from Economou, A., SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

Coverage of cybersecurity domain in SELFIEforTeachers



SELFIEforTEACHERS items

PROFESSIONAL ENGAGEMENT

- 1.1 Organisational communication
- 1.2 Online learning environments
- 1.3 Professional collaboration
- 1.4 Digital technologies and school level infrastructure
- 1.5 Reflective practice
- 1.6 Digital life
- 1.7 Professional learning (through digital technologies)
- 1.8 Professional learning (about digital technologies)
- 1.9 Computational thinking

DIGITAL RESOURCES

- 2.1 Searching and selecting
- 2.2 Creating
- 2.3 Modifying
- 2.4 Managing and protecting
- 2.5 Sharing

TEACHING AND LEARNING

- 3.1 Teaching
- 3.2 Guidance
- 3.3 Collaborative learning
- 3.4 Self-regulated learning
- 3.5 Emerging technologies

ASSESSMENT

- 4.1 Assessment strategies
- 4.2 Analysing evidence
- 4.3 Feedback and planning

EMPOWERING LEARNERS

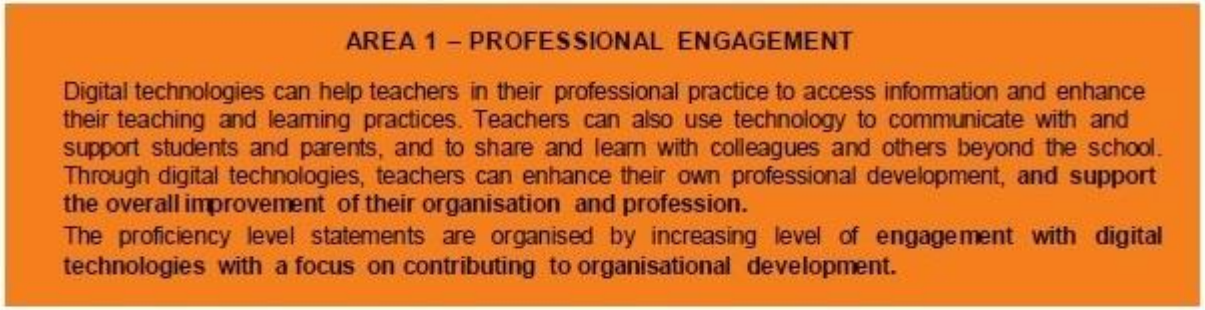
- 5.1 Accessibility and inclusion
- 5.2 Differentiation and personalisation
- 5.3 Actively engaging learners
- 5.4 Blended learning

FACILITATING LEARNERS' DIGITAL COMPETENCE

- 6.1 Information and data literacy
- 6.2 Communication and collaboration
- 6.3 Content creation
- 6.4 Safety and wellbeing
- 6.5 Responsible use
- 6.6 Problem solving

Fig. 7 - SELFIEforTeachers competence areas and items with cybersecurity-related competences highlighted[12]

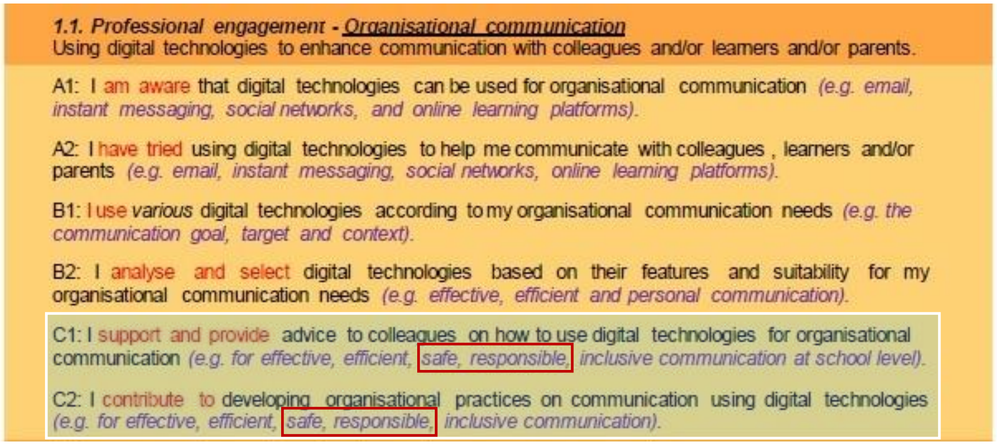
[12] Figure (and tables on following pages, with emphasis added) from Economou, A., SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699



AREA 1 – PROFESSIONAL ENGAGEMENT

Digital technologies can help teachers in their professional practice to access information and enhance their teaching and learning practices. Teachers can also use technology to communicate with and support students and parents, and to share and learn with colleagues and others beyond the school. Through digital technologies, teachers can enhance their own professional development, **and support the overall improvement of their organisation and profession.**

The proficiency level statements are organised by increasing level of **engagement with digital technologies with a focus on contributing to organisational development.**



1.1. Professional engagement - Organisational communication
Using digital technologies to enhance communication with colleagues and/or learners and/or parents.

A1: I am aware that digital technologies can be used for organisational communication *(e.g. email, instant messaging, social networks, and online learning platforms).*

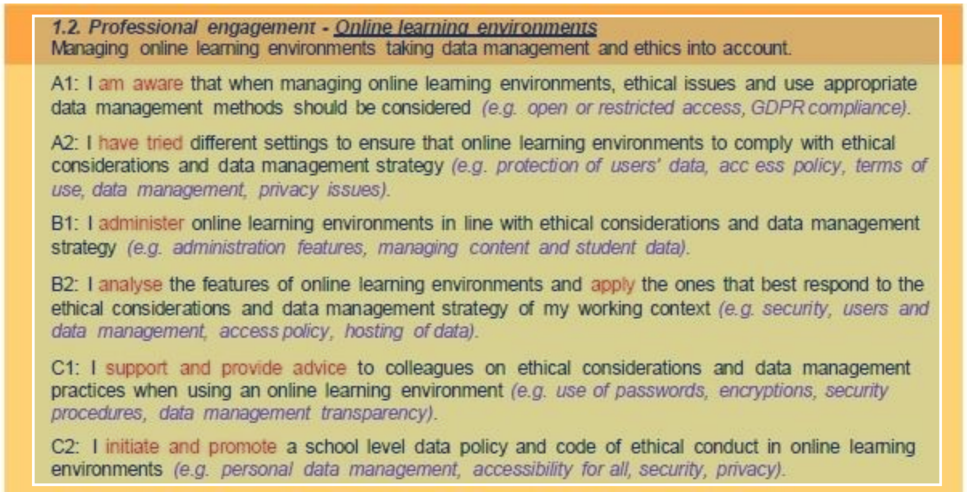
A2: I have tried using digital technologies to help me communicate with colleagues , learners and/or parents *(e.g. email, instant messaging, social networks, online learning platforms).*

B1: I use *various* digital technologies according to my organisational communication needs *(e.g. the communication goal, target and context).*

B2: I analyse and select digital technologies based on their features and suitability for my organisational communication needs *(e.g. effective, efficient and personal communication).*

C1: I support and provide advice to colleagues on how to use digital technologies for organisational communication *(e.g. for effective, efficient, safe, responsible, inclusive communication at school level).*

C2: I contribute to developing organisational practices on communication using digital technologies *(e.g. for effective, efficient, safe, responsible, inclusive communication).*



1.2. Professional engagement - Online learning environments
Managing online learning environments taking data management and ethics into account.

A1: I am aware that when managing online learning environments, ethical issues and use appropriate data management methods should be considered *(e.g. open or restricted access, GDPR compliance).*

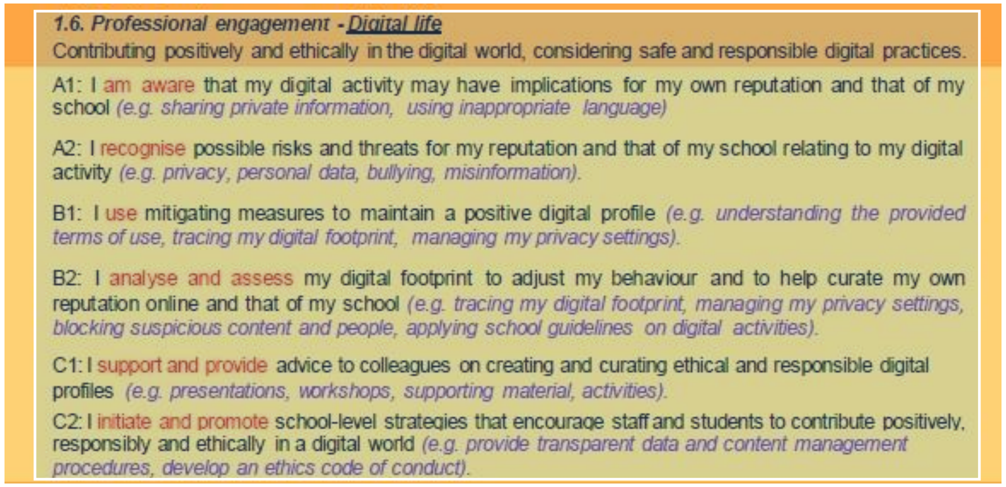
A2: I have tried different settings to ensure that online learning environments to comply with ethical considerations and data management strategy *(e.g. protection of users' data, acc ess policy, terms of use, data management, privacy issues).*

B1: I administer online learning environments in line with ethical considerations and data management strategy *(e.g. administration features, managing content and student data).*

B2: I analyse the features of online learning environments and apply the ones that best respond to the ethical considerations and data management strategy of my working context *(e.g. security, users and data management, access policy, hosting of data).*

C1: I support and provide advice to colleagues on ethical considerations and data management practices when using an online learning environment *(e.g. use of passwords, encryptions, security procedures, data management transparency).*

C2: I initiate and promote a school level data policy and code of ethical conduct in online learning environments *(e.g. personal data management, accessibility for all, security, privacy).*



1.6. Professional engagement - Digital life
Contributing positively and ethically in the digital world, considering safe and responsible digital practices.

A1: I am aware that my digital activity may have implications for my own reputation and that of my school *(e.g. sharing private information, using inappropriate language)*

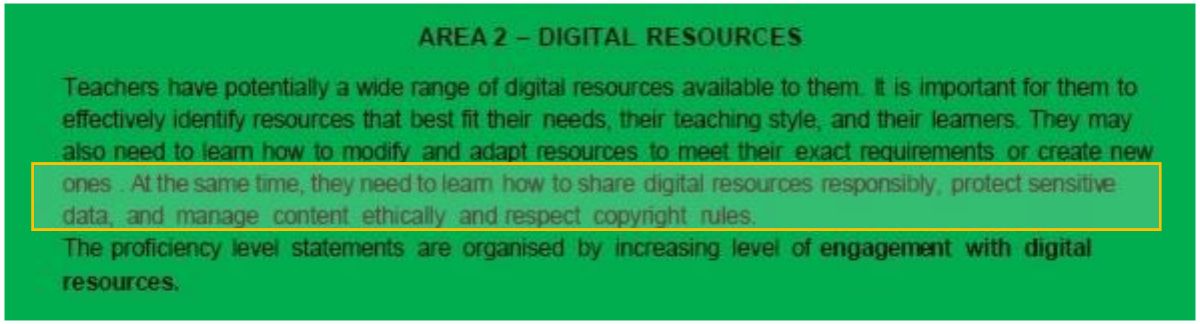
A2: I recognise possible risks and threats for my reputation and that of my school relating to my digital activity *(e.g. privacy, personal data, bullying, misinformation).*

B1: I use mitigating measures to maintain a positive digital profile *(e.g. understanding the provided terms of use, tracing my digital footprint, managing my privacy settings).*

B2: I analyse and assess my digital footprint to adjust my behaviour and to help curate my own reputation online and that of my school *(e.g. tracing my digital footprint, managing my privacy settings, blocking suspicious content and people, applying school guidelines on digital activities).*

C1: I support and provide advice to colleagues on creating and curating ethical and responsible digital profiles *(e.g. presentations, workshops, supporting material, activities).*

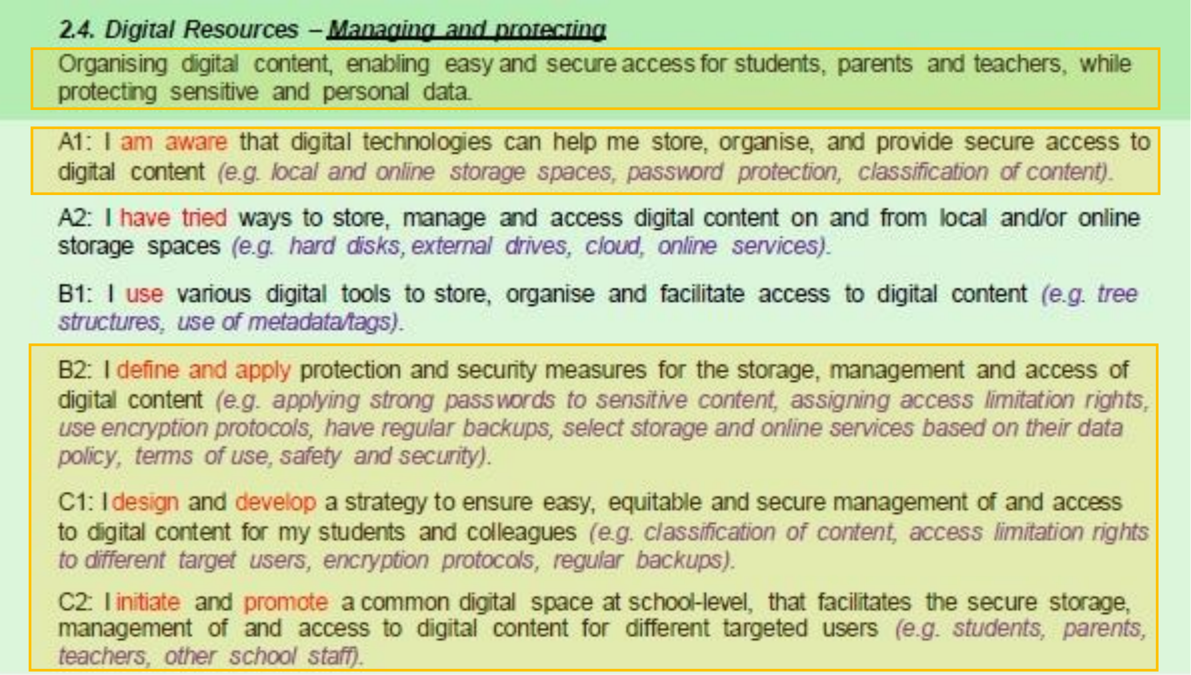
C2: I initiate and promote school-level strategies that encourage staff and students to contribute positively, responsibly and ethically in a digital world *(e.g. provide transparent data and content management procedures, develop an ethics code of conduct).*



AREA 2 – DIGITAL RESOURCES

Teachers have potentially a wide range of digital resources available to them. It is important for them to effectively identify resources that best fit their needs, their teaching style, and their learners. They may also need to learn how to modify and adapt resources to meet their exact requirements or create new ones . At the same time, they need to learn how to share digital resources responsibly, protect sensitive data, and manage content ethically and respect copyright rules.

The proficiency level statements are organised by increasing level of **engagement with digital resources.**



2.4. Digital Resources – __Managing and protecting__

Organising digital content, enabling easy and secure access for students, parents and teachers, while protecting sensitive and personal data.

A1: I am aware that digital technologies can help me store, organise, and provide secure access to digital content *(e.g. local and online storage spaces, password protection, classification of content).*

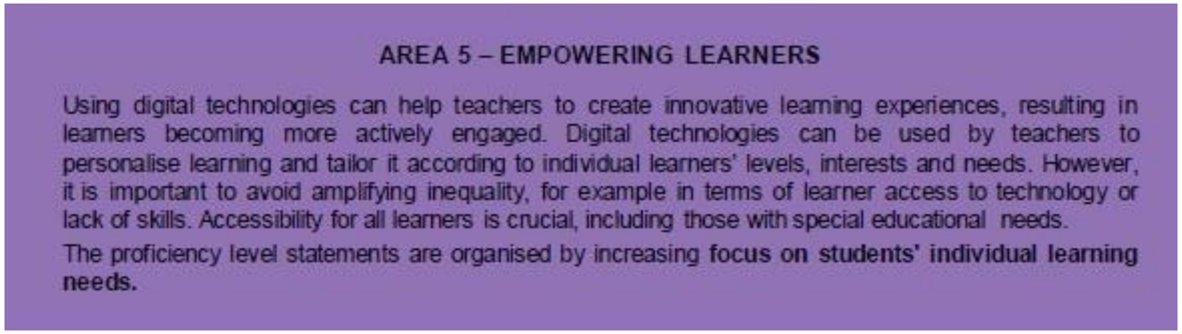
A2: I have tried ways to store, manage and access digital content on and from local and/or online storage spaces *(e.g. hard disks, external drives, cloud, online services).*

B1: I use various digital tools to store, organise and facilitate access to digital content *(e.g. tree structures, use of metadata/tags).*

B2: I define and apply protection and security measures for the storage, management and access of digital content *(e.g. applying strong passwords to sensitive content, assigning access limitation rights, use encryption protocols, have regular backups, select storage and online services based on their data policy, terms of use, safety and security).*

C1: I design and develop a strategy to ensure easy, equitable and secure management of and access to digital content for my students and colleagues *(e.g. classification of content, access limitation rights to different target users, encryption protocols, regular backups).*

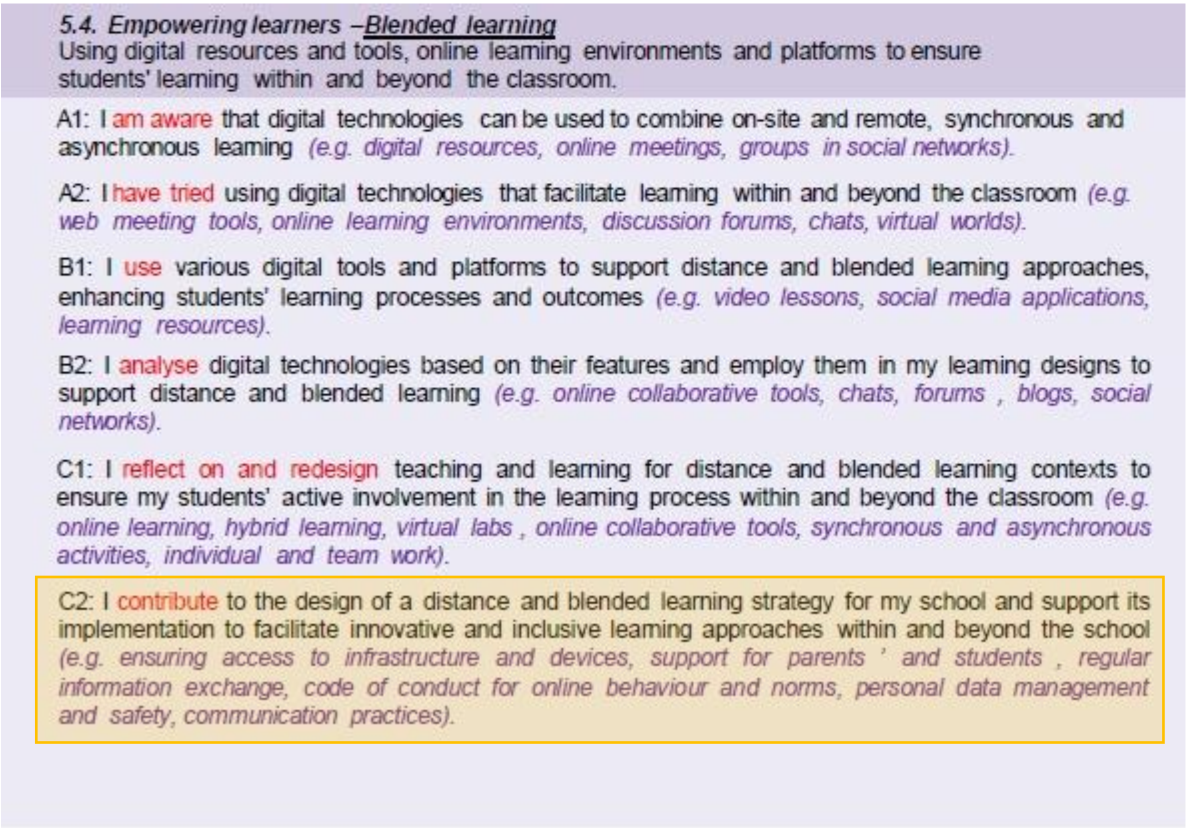
C2: I initiate and promote a common digital space at school-level, that facilitates the secure storage, management of and access to digital content for different targeted users *(e.g. students, parents, teachers, other school staff).*



AREA 5 – EMPOWERING LEARNERS

Using digital technologies can help teachers to create innovative learning experiences, resulting in learners becoming more actively engaged. Digital technologies can be used by teachers to personalise learning and tailor it according to individual learners' levels, interests and needs. However, it is important to avoid amplifying inequality, for example in terms of learner access to technology or lack of skills. Accessibility for all learners is crucial, including those with special educational needs.

The proficiency level statements are organised by increasing **focus on students' individual learning needs.**



5.4. Empowering learners –__Blended learning__
Using digital resources and tools, online learning environments and platforms to ensure students' learning within and beyond the classroom.

A1: I am aware that digital technologies can be used to combine on-site and remote, synchronous and asynchronous learning *(e.g. digital resources, online meetings, groups in social networks).*

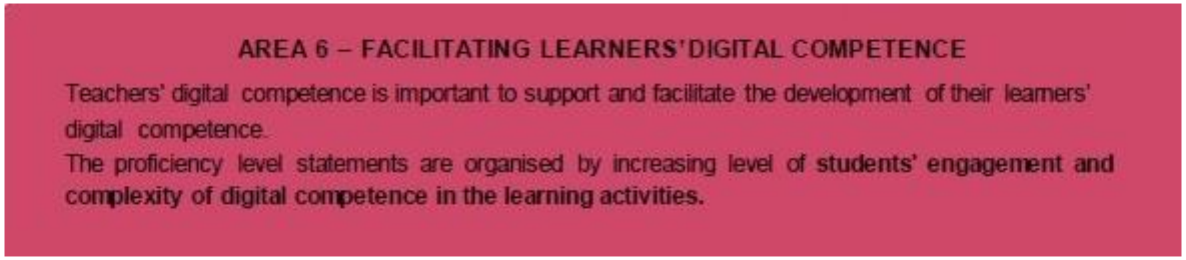
A2: I have tried using digital technologies that facilitate learning within and beyond the classroom *(e.g. web meeting tools, online learning environments, discussion forums, chats, virtual worlds).*

B1: I use various digital tools and platforms to support distance and blended learning approaches, enhancing students' learning processes and outcomes *(e.g. video lessons, social media applications, learning resources).*

B2: I analyse digital technologies based on their features and employ them in my learning designs to support distance and blended learning *(e.g. online collaborative tools, chats, forums , blogs, social networks).*

C1: I reflect on and redesign teaching and learning for distance and blended learning contexts to ensure my students' active involvement in the learning process within and beyond the classroom *(e.g. online learning, hybrid learning, virtual labs , online collaborative tools, synchronous and asynchronous activities, individual and team work).*

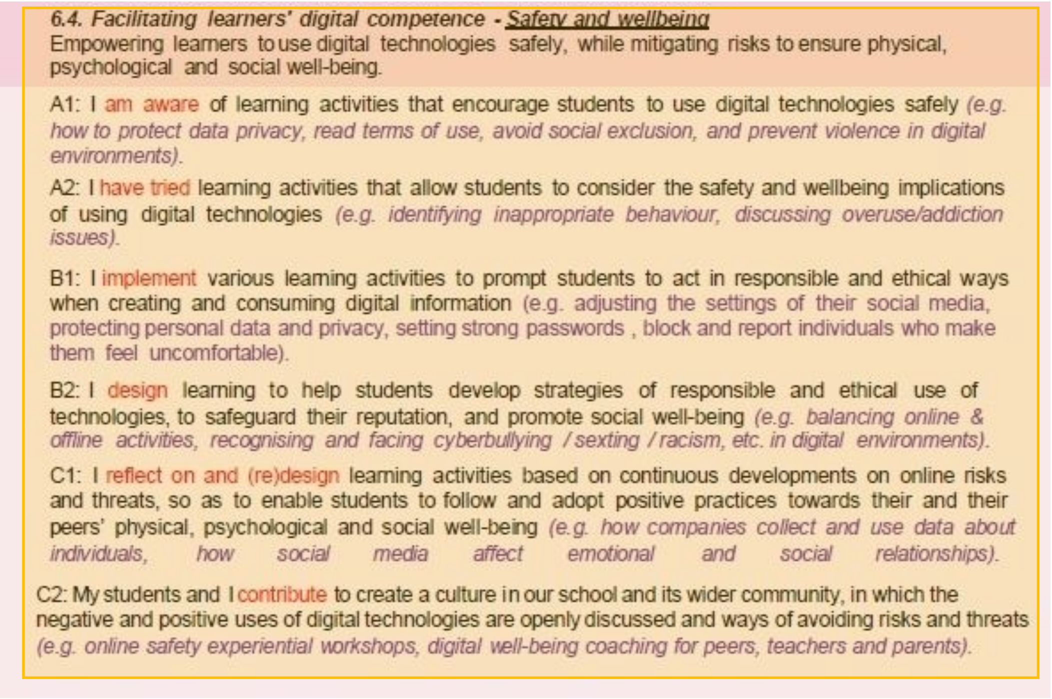
C2: I contribute to the design of a distance and blended learning strategy for my school and support its implementation to facilitate innovative and inclusive learning approaches within and beyond the school *(e.g. ensuring access to infrastructure and devices, support for parents ' and students , regular information exchange, code of conduct for online behaviour and norms, personal data management and safety, communication practices).*



AREA 6 – FACILITATING LEARNERS' DIGITAL COMPETENCE

Teachers' digital competence is important to support and facilitate the development of their learners' digital competence.

The proficiency level statements are organised by increasing level of **students' engagement and complexity of digital competence in the learning activities.**



6.4. Facilitating learners' digital competence - ***Safety and wellbeing***

Empowering learners to use digital technologies safely, while mitigating risks to ensure physical, psychological and social well-being.

A1: I am aware of learning activities that encourage students to use digital technologies safely *(e.g. how to protect data privacy, read terms of use, avoid social exclusion, and prevent violence in digital environments).*

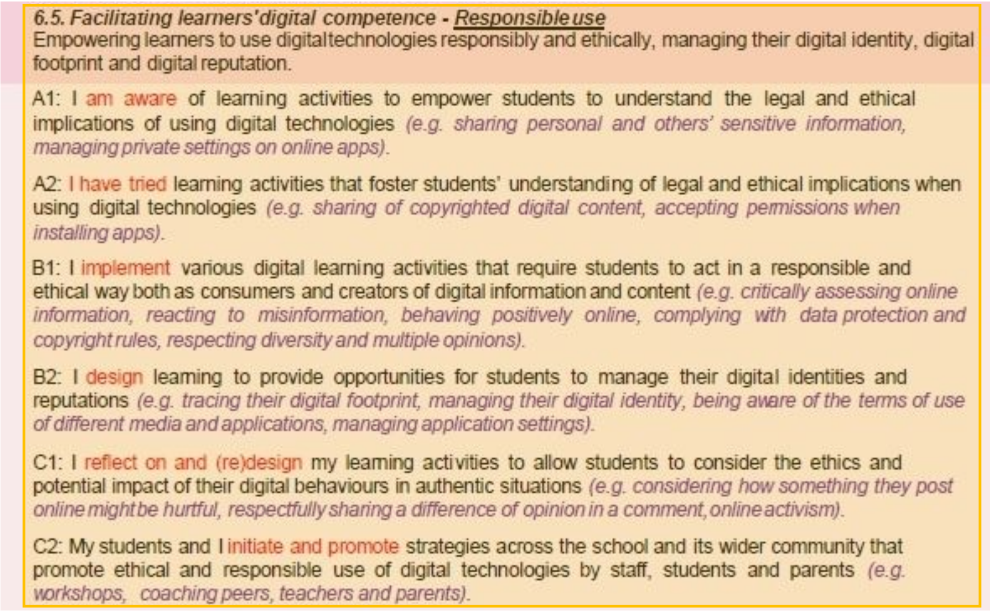
A2: I have tried learning activities that allow students to consider the safety and wellbeing implications of using digital technologies *(e.g. identifying inappropriate behaviour, discussing overuse/addiction issues).*

B1: I implement various learning activities to prompt students to act in responsible and ethical ways when creating and consuming digital information (e.g. adjusting the settings of their social media, protecting personal data and privacy, setting strong passwords , block and report individuals who make them feel uncomfortable).

B2: I design learning to help students develop strategies of responsible and ethical use of technologies, to safeguard their reputation, and promote social well-being *(e.g. balancing online & offline activities, recognising and facing cyberbullying / sexting / racism, etc. in digital environments).*

C1: I reflect on and (re)design learning activities based on continuous developments on online risks and threats, so as to enable students to follow and adopt positive practices towards their and their peers' physical, psychological and social well-being *(e.g. how companies collect and use data about individuals, how social media affect emotional and social relationships).*

C2: My students and I contribute to create a culture in our school and its wider community, in which the negative and positive uses of digital technologies are openly discussed and ways of avoiding risks and threats *(e.g. online safety experiential workshops, digital well-being coaching for peers, teachers and parents).*



6.5. Facilitating learners' digital competence - ***Responsible use***

Empowering learners to use digital technologies responsibly and ethically, managing their digital identity, digital footprint and digital reputation.

A1: I am aware of learning activities to empower students to understand the legal and ethical implications of using digital technologies *(e.g. sharing personal and others' sensitive information, managing private settings on online apps).*

A2: I have tried learning activities that foster students' understanding of legal and ethical implications when using digital technologies *(e.g. sharing of copyrighted digital content, accepting permissions when installing apps).*

B1: I implement various digital learning activities that require students to act in a responsible and ethical way both as consumers and creators of digital information and content *(e.g. critically assessing online information, reacting to misinformation, behaving positively online, complying with data protection and copyright rules, respecting diversity and multiple opinions).*

B2: I design learning to provide opportunities for students to manage their digital identities and reputations *(e.g. tracing their digital footprint, managing their digital identity, being aware of the terms of use of different media and applications, managing application settings).*

C1: I reflect on and (re)design my learning activities to allow students to consider the ethics and potential impact of their digital behaviours in authentic situations *(e.g. considering how something they post online might be hurtful, respectfully sharing a difference of opinion in a comment, online activism).*

C2: My students and I initiate and promote strategies across the school and its wider community that promote ethical and responsible use of digital technologies by staff, students and parents *(e.g. workshops, coaching peers, teachers and parents).*

3. EC GUIDES TO BLENDED LEARNING IN THE COVID-19 ERA

3.1. Blended Learning for High Quality and Inclusive Primary and Secondary Education – Handbook

3.2. Blended learning in school education – guidelines for the start of the academic year 2020/21

Guidelines/handbook	Blended learning for high quality and inclusive primary and secondary education – Handbook	Blended learning in school education – guidelines for the start of the academic year 2020/21
Versioning	v1 (2021)	v1 (2020)
Description	*"This Staff Working Document is designed to accompany and support the Recommendation on blended learning for high quality and inclusive primary and secondary education. It provides research evidence and other information as a basis for both the legal text of the Recommendation and its subsequent supportive actions. It is also, as far as possible at the time of writing [the COVID-19 crisis], a practical guide/handbook to help stakeholders understand the full potential of this topic and to support real and positive change across systems and across Europe"*	Guide to blended learning published by the EC to support schools' efforts in coping successfully with the COVID-19 crisis and, in many cases, Emergency Remote Teaching.
Primary target	educational stakeholders and policy makers dealing with primary and secondary schools	Schools; educational stakeholders and policy makers

guidelines/handbook (cont.)	Blended learning for high quality and inclusive primary and secondary education – Handbook	Blended learning in school education – guidelines for the start of the academic year 2020/21
organisation & structure	Working document with examples of practice and recommendations. Includes a "Framework for Blended Learning" (p. 157) comprising a definition of blended learning and relevant policy measures, namely: (1) equal right of all learners; 2) system-wide approach; 3) supporting educators; 4) collaboration; 5) access; 6) well-being; 7) digital technology and content; 8) curricula and assessment; 9) school strategy and leadership; 10) monitoring. Each of these contains observations/recommendations, plus a set of good practices for adoption.	"Successful Blending Learning" framed in eight thematic areas ("Key Considerations"): School leadership; Legislation to support decision making; Managing in-school and distance learning environments for all learners; Teachers - role, competences and working conditions; Learner assessment; Well-being of staff and pupils; Collaboration and school community; Quality assurance; Evaluation and feedback. Each of these groups a set of sub-considerations potentially transformable into "guiding questions for stakeholders, for example: "Does our system have in place…?" or "How can our schools…?"
cybersecurity coverage	Indications on need for safe and secure use of digital environments/tools; learner wellbeing (cyberbullying); school application of data protection rules for children	"Well-being of staff & pupils" features as one of the eight Thematic Area with related key considerations (e.g. anxiety/stress caused by cyberbullying). Safe and secure use of digital environments/tools addressed.
repository	https://data.europa.eu/doi/10.2766/237842	https://www.schooleducationgateway.eu/en/pub/resources/publications/blended-learning-guidelines.htm
main EC publications	European Commission, Directorate-General for Education, Youth, Sport and Culture, Blended learning for high quality and inclusive primary and secondary education – Handbook, Publications Office of the European Union, 2021, https://data.europa.eu/doi/10.2766/237842	European Commission, Directorate-General Education, Youth, Sport and Culture, Unit B.2: Schools and multilingualism (2020). Blended learning in school education – guidelines for the start of the academic year 2020/21. Available at: https://www.schooleducationgateway.eu/downloads/Blended%20learning%20in%20school%20education_European%20Commission_June%202020.pdf (retrieved May 2023)

Coverage of cybersecurity domain in EC guides to blended learning

From "Blended learning for high quality and inclusive primary and secondary education – Handbook" (EC, 2021)

2.5 LEARNERS AND BLENDED LEARNING

Specific needs relating to environments and tools

……

- *a safe and secure online experience for pupils of all ages when connecting with digital devices …….*

3.2.1 Design and management of learning

Attitudes and concerns relating to the use of digital tools

……..

Digital tools

…..Any web-based tools or platforms should be suitable and relevant to pupils' age as well as intuitional and user friendly. Data collection should be compliant with data protection rules. …..For the safety of learners, it may be necessary to review the set-up of secure passwords and logins as well as filters for the use of internet content. IT Infrastructure providers offer many security options and filters that allow educators to block problematic apps and websites.

3.2.4 Well-being of staff and pupils

Identifying causes of anxiety and stress:

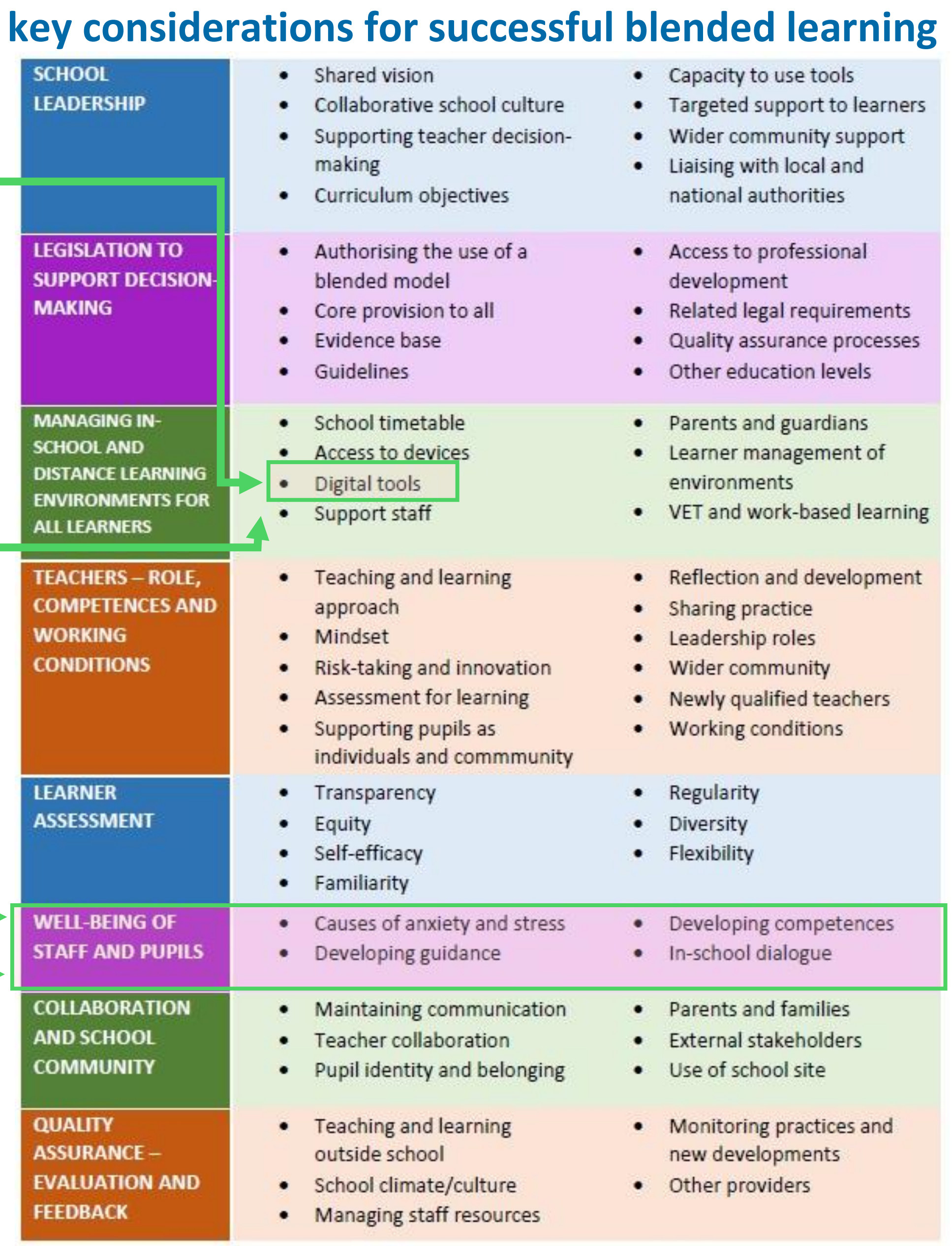
………..

- *Loss of a 'safe' place away from difficult or dangerous home environments for some children;*
- *Extended exposures to digital screens or stress caused by cyber-bullying.*

[Recommendation]

Simply identifying the possible causes is the first step to developing ways to prevent, mitigate or overcome such problems.

From "Blended learning in school education – guidelines for the start of the academic year 2020-2022" (EC, 2020)



key considerations for successful blended learning

SCHOOL LEADERSHIP	• Shared vision • Collaborative school culture • Supporting teacher decision-making • Curriculum objectives	• Capacity to use tools • Targeted support to learners • Wider community support • Liaising with local and national authorities
LEGISLATION TO SUPPORT DECISION-MAKING	• Authorising the use of a blended model • Core provision to all • Evidence base • Guidelines	• Access to professional development • Related legal requirements • Quality assurance processes • Other education levels
MANAGING IN-SCHOOL AND DISTANCE LEARNING ENVIRONMENTS FOR ALL LEARNERS	• School timetable • Access to devices • Digital tools • Support staff	• Parents and guardians • Learner management of environments • VET and work-based learning
TEACHERS – ROLE, COMPETENCES AND WORKING CONDITIONS	• Teaching and learning approach • Mindset • Risk-taking and innovation • Assessment for learning • Supporting pupils as individuals and commmunity	• Reflection and development • Sharing practice • Leadership roles • Wider community • Newly qualified teachers • Working conditions
LEARNER ASSESSMENT	• Transparency • Equity • Self-efficacy • Familiarity	• Regularity • Diversity • Flexibility
WELL-BEING OF STAFF AND PUPILS	• Causes of anxiety and stress • Developing guidance	• Developing competences • In-school dialogue
COLLABORATION AND SCHOOL COMMUNITY	• Maintaining communication • Teacher collaboration • Pupil identity and belonging	• Parents and families • External stakeholders • Use of school site
QUALITY ASSURANCE – EVALUATION AND FEEDBACK	• Teaching and learning outside school • School climate/culture • Managing staff resources	• Monitoring practices and new developments • Other providers

....

Developing guidance for the whole school community

....

- *A positive use and personal management of digital tools and social media; and supporting the application of data protection rules to children*

1.2.3 MANAGING THE IN-SCHOOL AND DISTANCE LEARNING ENVIRONMENTS TO SUPPORT ALL LEARNERS

....

iii. Digital tools

......Data collection should be compliant with data protection rules.......For the safety of learners, it may be necessary to review the set-up of secure passwords and logins as well as filters for the use of internet content. IT Infrastructure providers offer many security options and filters that allow educators to block problematic apps and websites.

1.2.6 WELL-BEING OF STAFF & PUPILS

i. Identifying causes of anxiety and stress:

....

- *Loss of a 'safe' place away from difficult or dangerous home environments for some children;*

Extended exposures to digital screens or stress caused by cyber-bullying

[Recommendation]

Simply identifying the possible causes is the first step to developing ways to prevent, mitigate or overcome such problems.

....

4. EC PUBLICATIONS FOCUSING ON CYBERSECURITY MATTERS

4.1. **[ECSF]** - European Cybersecurity Skills Framework

framework	ECSF - European Cybersecurity Skills Framework (European Union Agency for Cybersecurity – ENISA)[13]
versioning	V1 (Sept 2022)
description	Descriptive taxonomy of professional profiles within the cybersecurity sector
primary target	Stakeholders and policy makers in the cybersecurity sector
organisation & structure	List of 12 professional profiles within the cybersecurity sector, each identified by a Profile Title and nine attributes: Alternative Title(s;) Summary statement; Mission; Deliverable(s); Main task(s); Key skill(s); Key knowledge; e-Competences [from e-CF - EN16234-1 e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors]
cybersecurity coverage	The entire taxonomy is devoted to cybersecurity, encompassing an industry-wide perspective. One of the 12 profiles, CYBERSECURITY EDUCATOR, is potentially of relevance to cybersecurity education in the school sector.
ENISA platform	https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
main EC publications	• European Union Agency for Cybersecurity (ENISA), (2022). *ECSF - European Cybersecurity Skills Framework*. ISBN: 978-92-9204-584-5 DOI: 10.2824/859537. © European Union Agency for Cybersecurity (ENISA), 2022 • European Union Agency for Cybersecurity (ENISA), (2022). *User Manual, ECSF - European Cybersecurity Skills Framework*. ISBN: 978-92-9204-583-8 – DOI: 10.2824/95989 © European Union Agency for Cybersecurity (ENISA), 2022[14] [note: this latter document addresses the educational perspective of cybersecurity at the levels of Vocational Education & Training (VET), Higher Education (HE), and workplace education & training. It therefore falls outside the scope of this review].

[13] The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. More information about ENISA and its work can be found here: www.enisa.europa.eu.

[14] This document addresses the educational perspective of cybersecurity at the levels of Vocational Education & Training (VET), Higher Education (HE), and workplace education & training. It therefore falls outside the scope of this survey.

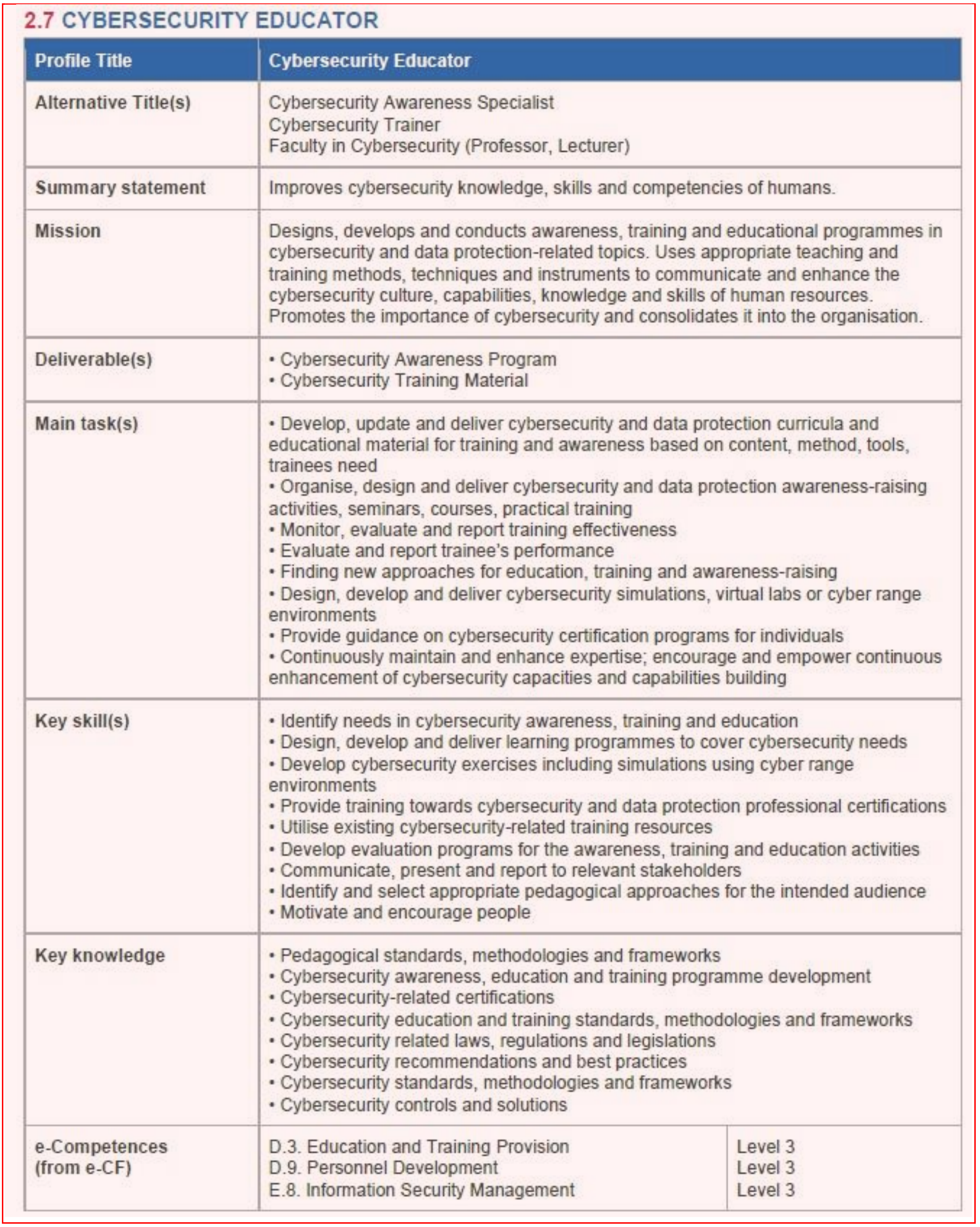
Organisational structure of ECSF

- **LIST OF PROFILES**
- **PROFILE TITLE**
- **Profile attributes** [Alternative Title(s;) Summary statement; Mission; Deliverable(s); Main task(s); Key skill(s); Key knowledge; e-Competences (from e-CF)]
- Attribute value [Descriptive text or bulleted list reifying each attribute]

Coverage of (school-related) cybersecurity domain in ECSF[15]

[15] Images on the following page from European Union Agency for Cybersecurity (ENISA), (2022). ECSF - European Cybersecurity Skills Framework. ISBN: 978-92-9204-584-5 DOI: 10.2824/859537. © European Union Agency for Cybersecurity (ENISA), 2022: emphasis added.

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester
01010
11101
00101
01
101



2.7 CYBERSECURITY EDUCATOR

Profile Title	Cybersecurity Educator	
Alternative Title(s)	Cybersecurity Awareness Specialist Cybersecurity Trainer Faculty in Cybersecurity (Professor, Lecturer)	
Summary statement	Improves cybersecurity knowledge, skills and competencies of humans.	
Mission	Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organisation.	
Deliverable(s)	• Cybersecurity Awareness Program • Cybersecurity Training Material	
Main task(s)	• Develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need • Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses, practical training • Monitor, evaluate and report training effectiveness • Evaluate and report trainee's performance • Finding new approaches for education, training and awareness-raising • Design, develop and deliver cybersecurity simulations, virtual labs or cyber range environments • Provide guidance on cybersecurity certification programs for individuals • Continuously maintain and enhance expertise; encourage and empower continuous enhancement of cybersecurity capacities and capabilities building	
Key skill(s)	• Identify needs in cybersecurity awareness, training and education • Design, develop and deliver learning programmes to cover cybersecurity needs • Develop cybersecurity exercises including simulations using cyber range environments • Provide training towards cybersecurity and data protection professional certifications • Utilise existing cybersecurity-related training resources • Develop evaluation programs for the awareness, training and education activities • Communicate, present and report to relevant stakeholders • Identify and select appropriate pedagogical approaches for the intended audience • Motivate and encourage people	
Key knowledge	• Pedagogical standards, methodologies and frameworks • Cybersecurity awareness, education and training programme development • Cybersecurity-related certifications • Cybersecurity education and training standards, methodologies and frameworks • Cybersecurity related laws, regulations and legislations • Cybersecurity recommendations and best practices • Cybersecurity standards, methodologies and frameworks • Cybersecurity controls and solutions	
e-Competences (from e-CF)	D.3. Education and Training Provision D.9. Personnel Development E.8. Information Security Management	Level 3 Level 3 Level 3

4.2 [What can schools do about bullying?] - EC factsheet

publication	“*What can schools do about bullying?*” (European Commission, Directorate-General for Education, Youth, Sport and Culture)
versioning	2023
description	infographic factsheet devoted to bullying & cyberbullying of students, with suggested actions that schools, parents and communities can take in response
primary target	Schools & school communities
organisation & structure	Two-page infographic factsheet with academic references and links to further resources on the topics presented.
cybersecurity coverage	Addresses the specific topic of cyberbullying as part of the broader issue of bullying of students
EC repository	https://data.europa.eu/doi/10.2766/809742
main EC publication	European Commission, Directorate-General for Education, Youth, Sport and Culture, What can schools do about bullying? -, Publications Office of the European Union, 2023, https://dx.doi.org/10.2766/809742 [16]

Coverage of cybersecurity domain in “What can schools do about bullying?”

[16] Inserted in the following pages: emphasis added.

European Commission

What can schools do about bullying?

Bullying happens when a student hurts another on purpose, this behaviour is done more than once over time, and one student has more power than the other (is physically stronger or more popular).

Types of bullying

Physical attacks	Emotional	Indirect	Attack on property	Cyberbullying
hitting, kicking, pushing	commenting nastily on someone's appearance, name-calling, spreading rumours, mocking	leaving someone out of games, deliberately not choosing or inviting them, telling others not to play with that person	stealing their lunch or their money, damaging clothing, hiding sportswear, throwing their bags around	emotional bullying using electronic devices, such as mobile phones

Incidence of bullying

Boys are more likely than girls to bully and cyberbully others

While the proportion of boys and girls who are victims of traditional bullying is similar, girls are more likely to be cyberbullied

Over 1 in 10 adolescents has been cyberbullied at least once in the past couple of months

Students' exposure to bullying has been increasing. For instance, across OECD countries the share of students who reported being bullied at least a few times a month increased by 4 percentage points between 2015 and 2018

As indicated in a recent report of a survey on the mental health of children and young people in Europe and Canada, (World Health Organisation, 2020, pp. 30-31)

OECD (2019), PISA 2018 Results (Volume III)

Signs and symptoms in victimised children

Short-term

Parents are often the first to notice immediate signs of distress such as:

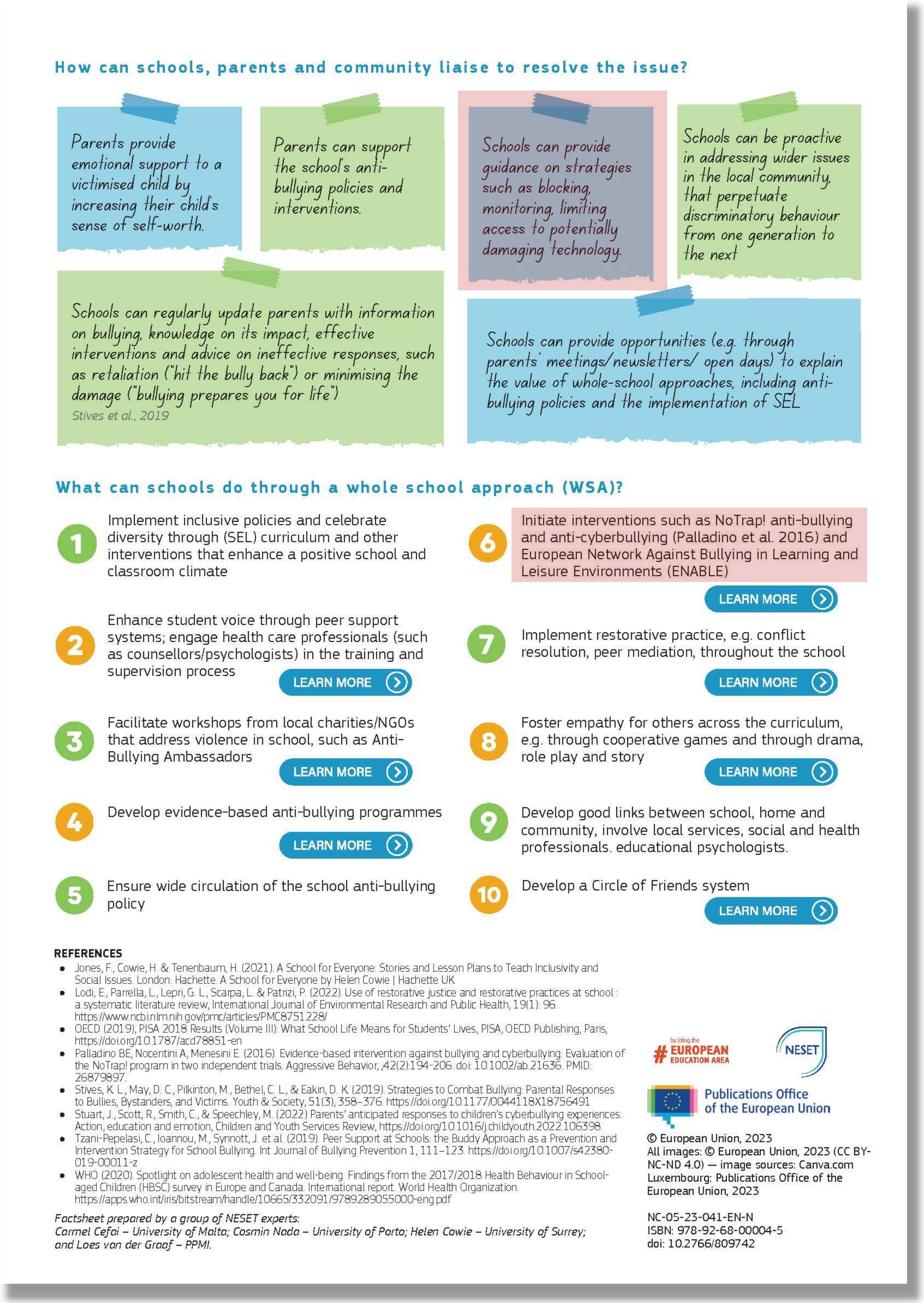
- Behaviour changes: child becomes moody, aggressive, angry
- Complains of stomach aches, headaches, sleeplessness
- Comes home with damaged or lost belongings
- Has unexplained injuries

Long-term

Over time, signs of continued bullying can be noticed by school professionals:

- Loss of confidence, becomes withdrawn
- Relationship difficulties, is isolated, mistrusts peer group
- Academic attainment drops
- At risk of mental health problems, such as depression and anxiety
- At risk of self-harm and suicidal ideation

Education and Training



How can schools, parents and community liaise to resolve the issue?

Parents provide emotional support to a victimised child by increasing their child's sense of self-worth.

Parents can support the school's anti-bullying policies and interventions.

Schools can provide guidance on strategies such as blocking, monitoring, limiting access to potentially damaging technology.

Schools can be proactive in addressing wider issues in the local community, that perpetuate discriminatory behaviour from one generation to the next

Schools can regularly update parents with information on bullying, knowledge on its impact, effective interventions and advice on ineffective responses, such as retaliation ("hit the bully back") or minimising the damage ("bullying prepares you for life")
Stives et al., 2019

Schools can provide opportunities (e.g. through parents' meetings/newsletters/ open days) to explain the value of whole-school approaches, including anti-bullying policies and the implementation of SEL

What can schools do through a whole school approach (WSA)?

1. Implement inclusive policies and celebrate diversity through (SEL) curriculum and other interventions that enhance a positive school and classroom climate
2. Enhance student voice through peer support systems; engage health care professionals (such as counsellors/psychologists) in the training and supervision process
   LEARN MORE
3. Facilitate workshops from local charities/NGOs that address violence in school, such as Anti-Bullying Ambassadors
   LEARN MORE
4. Develop evidence-based anti-bullying programmes
   LEARN MORE
5. Ensure wide circulation of the school anti-bullying policy
6. Initiate interventions such as NoTrap! anti-bullying and anti-cyberbullying (Palladino et al. 2016) and European Network Against Bullying in Learning and Leisure Environments (ENABLE)
   LEARN MORE
7. Implement restorative practice, e.g. conflict resolution, peer mediation, throughout the school
   LEARN MORE
8. Foster empathy for others across the curriculum, e.g. through cooperative games and through drama, role play and story
   LEARN MORE
9. Develop good links between school, home and community, involve local services, social and health professionals. educational psychologists.
10. Develop a Circle of Friends system
   LEARN MORE

REFERENCES

- Jones, F., Cowie, H. & Tenenbaum, H. (2021). A School for Everyone: Stories and Lesson Plans to Teach Inclusivity and Social Issues. London: Hachette. A School for Everyone by Helen Cowie | Hachette UK
- Lodi, E., Parrella, L., Lepri, G. L., Scarpa, L. & Patrizi, P. (2022). Use of restorative justice and restorative practices at school : a systematic literature review, International Journal of Environmental Research and Public Health, 19(1): 96. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8751228/
- OECD (2019), PISA 2018 Results (Volume III): What School Life Means for Students' Lives, PISA, OECD Publishing, Paris, https://doi.org/10.1787/acd78851-en
- Palladino BE, Nocentini A, Menesini E. (2016). Evidence-based intervention against bullying and cyberbullying: Evaluation of the NoTrap! program in two independent trials. Aggressive Behavior, ;42(2):194-206. doi: 10.1002/ab.21636. PMID: 26879897.
- Stives, K. L., May, D. C., Pilkinton, M., Bethel, C. L., & Eakin, D. K. (2019). Strategies to Combat Bullying: Parental Responses to Bullies, Bystanders, and Victims. Youth & Society, 51(3), 358–376. https://doi.org/10.1177/0044118X18756491
- Stuart, J., Scott, R., Smith, C., & Speechley, M. (2022) Parents' anticipated responses to children's cyberbullying experiences: Action, education and emotion, Children and Youth Services Review, https://doi.org/10.1016/j.childyouth.2022.106398
- Tzani-Pepelasi, C., Ioannou, M., Synnott, J. et al. (2019). Peer Support at Schools: the Buddy Approach as a Prevention and Intervention Strategy for School Bullying. Int Journal of Bullying Prevention 1, 111–123. https://doi.org/10.1007/s42380-019-00011-z
- WHO (2020). Spotlight on adolescent health and well-being. Findings from the 2017/2018 Health Behaviour in School-aged Children (HBSC) survey in Europe and Canada. International report. World Health Organization. https://apps.who.int/iris/bitstream/handle/10665/332091/9789289055000-eng.pdf

Factsheet prepared by a group of NESET experts:
Carmel Cefai – University of Malta; Cosmin Nada – University of Porto; Helen Cowie – University of Surrey; and Loes van der Graaf – PPMI.

building the # EUROPEAN EDUCATION AREA

NESET

Publications Office of the European Union

Luxembourg: Publications Office of the European Union, 2023

NC-05-23-041-EN-N
ISBN: 978-92-68-00004-5
doi: 10.2766/809742

5. DISCUSSION & FINAL CONSIDERATIONS

This study brings to light considerable variation in how cybersecurity-related issues are treated in the surveyed frameworks, self-assessment tools and guides on digital competence/capacity in education developed by - and produced under the auspices of - the European Commission (EC). This variation is particularly apparent in the positioning and granularity with which cybersecurity matters are treated as part of digital competence/capacity generally, and also to some extent in the nature of that treatment. This variance can largely be attributed to the fact that the surveyed initiatives (a) are intended for different purposes (conceptual framing, functional self-assessment, practical guidance); (b) concern the digital competence/capacity of quite different target groups (individuals/citizens, school communities, teachers); and (c) are designed for different stakeholder groups (educational authorities, policy makers, researchers, school leaders, practitioners, etc.).

In any case, it is also worth noting how digital competence/capacity in education (and cybersecurity matters as a constituent part of that) continues to be a high priority for the EC. This is borne out in ongoing development, updating and expansion of initiatives like **DigComp 2.2** and related support material, the **SELFIE/SELFIEforTeachers** tools and related ecosystems, and EC support for **Blended Learning/Emergency Remote Teaching** during the COVID-19 pandemic. Increasing priority devoted to cybersecurity competences – professionally and in education - is clearly manifest in the surveyed initiatives **European Cybersecurity Skills Framework** and the EC factsheet, **"What can schools do about bullying"**, but also in funding of cybersecurity-in-education projects such as SuperCyberKids itself.

5.1. Coverage of the cybersecurity domain

Two separate analyses were performed on the cybersecurity-related content aggregated from the nine surveyed digital competence frameworks, self-assessment tools and guides (Sections 2 to 5). The first analysis was essentially carried out to scope coverage of cybersecurity in these EC documents. In this case, standard productivity suite applications and free online text processing tools were employed. In addition, some semantic filtering and clustering was performed manually, with personal subjectivity came into play. A second, more automated, analysis was carried out using T-LAB software (Lancia, 2004), a dedicated text analysis tool, to gain insights into the semantic relations in the dataset between the core concept "security" and other lemma (individual words) or collocations (commonly combined word combinations like "digital environment"). Together, the two analyses give a sense of the breadth, depth and nature of cybersecurity coverage in the aforementioned EC document sources.

The findings reported here complement and intersect with those from the other desktop studies and field investigations performed in the SuperCyberKids project for defining the "SuperCyberKids Skills Framework" (SCKSF - see Section 1). Examining cybersecurity from different perspectives - academic literature, stakeholder/expert views, implemented educational initiatives, [digital] educational policy-making - can only help to enrich and strengthen the framework, instilling it with greater potential applicability throughout the ecosystem it will be situated in.

Scoping analysis

As described in the table below, steps were performed to extract and distil a dataset of cybersecurity terminology from the identified cybersecurity content reported in Sections 2 to 5.

***Table 1** - steps for extracting/distilling cybersecurity terminology dataset from surveyed EC sources (Sections 2 to 5)*

STEPS	ACTION PERFORMED	TOOLS EMPLOYED[17]	OUTPUT
1	All cybersecurity-related textual content reported in Sections 2-5 extracted and aggregated	Adobe Acrobat & Microsoft Word (manual copy & paste)	raw block of contextual text passages = **6258** words
2	Manual congruency processing of raw text-block[18]	Microsoft Word	Semi-refined block of contextual text passages = **5826** words

[17] The free-access online text processing tools employed do not guarantee 100% accuracy, so some minor discrepancies are foreseeable.

[18] Contextual removal of repeated/irrelevant framework structure headings, subheadings & labels/identifiers (e.g. "Use Cases", "Employment Scenario", "Advanced level 5", etc). In addition, two context-reliant syntactic uniformity adjustments were made: (i) [well-being/well being] = "wellbeing"; (ii) [cyber bull*/cyber-bull*] = "cyberbull*" (rationale: both "well" and "cyber" are prefixes for other composite terms in the dataset)

STEPS CONT.	ACTION PERFORMED CONT.	TOOLS EMPLOYED CONT.	OUTPUT CONT.
3	Semi-refined text block converted into dataset (word lists)	https://www.browserling.com/tools/word-frequency	ordered lists of single word instances & their numerical frequency value
4	Minor congruency processing performed on dataset[19]	Microsoft Excel & Microsoft Word	list of **1099** distinct lemmas with multiple instances = **5808** word dataset
5	dataset fed into online word-cloud generators	https://www.freewordcloudgenerator.com https://tagcrowd.com	Word-clouds shown in figs.8 & 9
6	Subjective/manual identification of cybersecurity terms in dataset	Microsoft Excel & Microsoft Word	List of cybersecurity terms, including their root (lemma) and set of inflected/alternate forms (lexeme)
7	Semantic clustering of 'flagbearer' cybersecurity terms, labelled by highest-instance frequency[20]	Microsoft Excel	Dataset of cybersecurity terms distilled from Step 4 dataset = **22** cybersecurity lemma; **594** instances[21]
8	Distilled cybersecurity dataset of instances fed into word-cloud generator	https://www.freewordcloudgenerator.com https://tagcrowd.com	Distilled word-cloud of cybersecurity terms shown in figs. 10 & 11

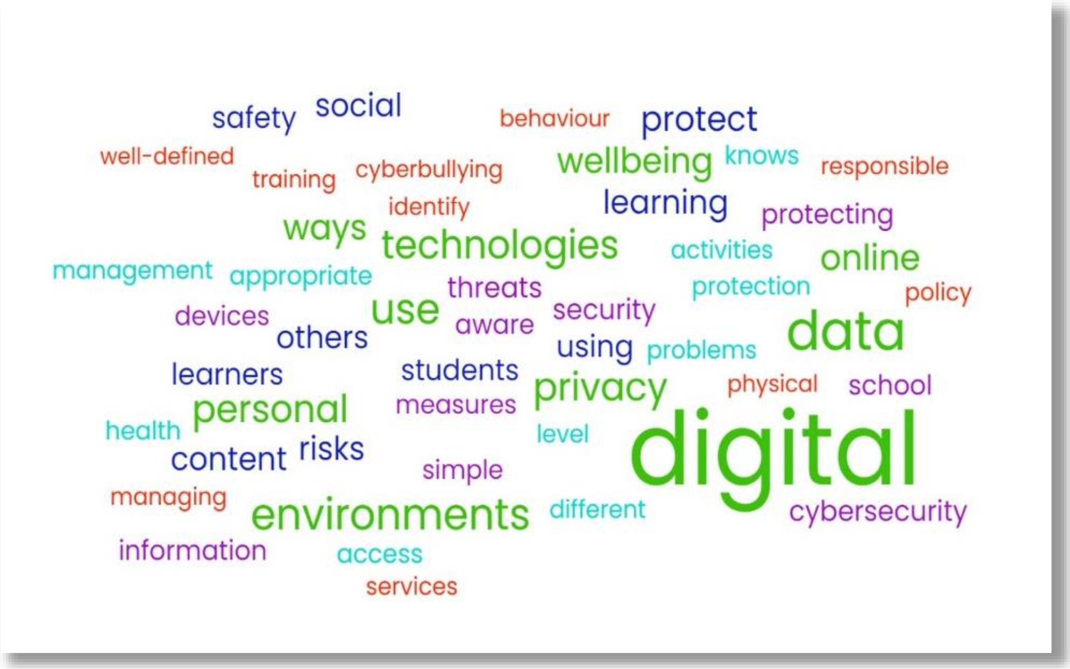


***Fig. 9** – Step 5 output: word cloud generated from aggregated content extracted from the surveyed EC publications & tools (https://www.freewordcloudgenerator.com)*

[19] removal of invalid instances: punctuation marks, numbers, non-values, etc.

[20] For example, clustering of the terms **cybersecurity** (25 instances) + **security** (25) + **secure** (8) + **cybersecurity-related** (2) + **securely** (1). Assigned cluster label = **cybersecurity** (due to highest frequency in cluster). One instance of collocation clustering was also applied to a cluster label ("personal" + "data" = "personal-data") as the online word cloud generator automatically treated these as separate lemmas.

[21] protect (81); cyber-security (61); privacy (52); safety (48); personal-data (42); wellbeing (40); risks (37); aware (35); cyberbullying (30); threats (28); appropriate (28); responsible (26); health (21); dangers (16); passwords (14); identity (11); sensitive (7); malware (4); victims (4); confidentiality (3); authentication (3); GDPR (3).

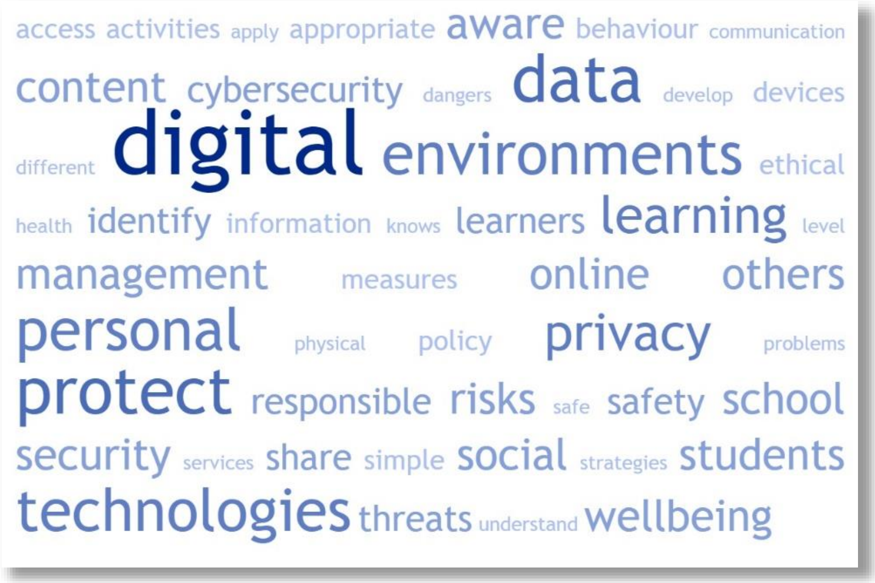


Fig. 10 *– Step 5 output: word cloud in alphabetical order generated from aggregated content extracted from the surveyed EC publications & tools (https://tagcrowd.com)*

Examining the two Step 5 word clouds (figs. 8 & 9) through the lens of the cybersecurity domain, the most striking result to emerge is the prominence in both clouds of the terms “protect”, “privacy” and “personal” (data/information), “wellbeing”, “risks” and (to a lesser extent) “[cyber]security” itself.

These terms also emerge strongly from the Step 7 semantic clustering of the cybersecurity terms subjectively selected in Step 6, as demonstrated both by the resulting Step 8 word clouds (figs. 10 & 11) and the list of 22 cybersecurity terms themselves (listed in Step 7 footnote). As a result of the clustering process, “cybersecurity” gains greater prominence, as do “safety”, cyberbullying”, “aware”, “threats”, “appropriate” and “responsible”.

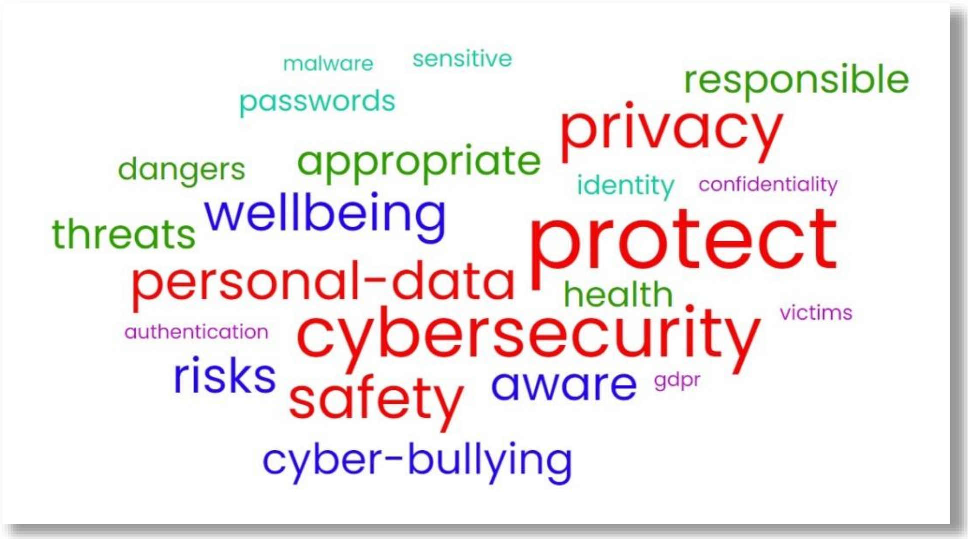


Fig. 11 *- Step 8 output: word cloud generated from extracted ‘flagbearer’ cybersecurity-domain terms (https://www.freewordcloudgenerator.com)*

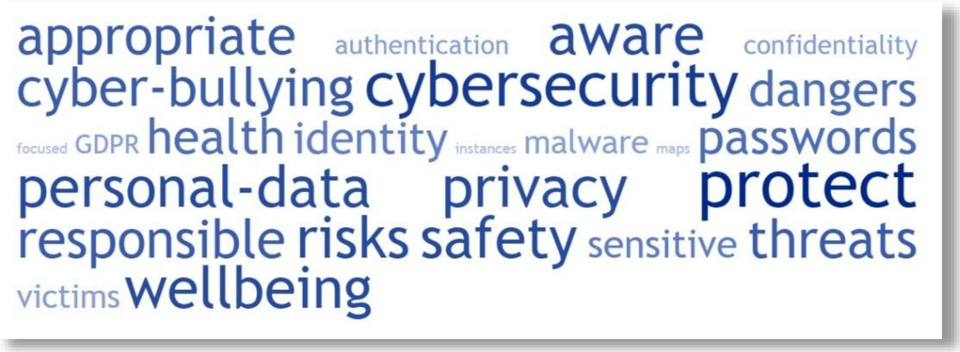


Fig. 12 - Step 8 output: word cloud in alphabetical order generated from extracted 'flagbearer' cybersecurity-domain terms (https://tagcrowd.com)

Relational "SECURITY" centred analysis

The brevity of the aggregated corpus in this survey did not allow application of full quantitative analysis. However, T-LAB software (Lancia, 2004) – along with a set of linguistic, statistical and graphical tools – were adopted to conduct some analytical investigation of an exploratory nature. Specifically, the "Word Associations" function was employed on the lemma "SECURITY" (Fig. 12) to explore its co-occurrence relationships, which determine its 'contextual meaning'.

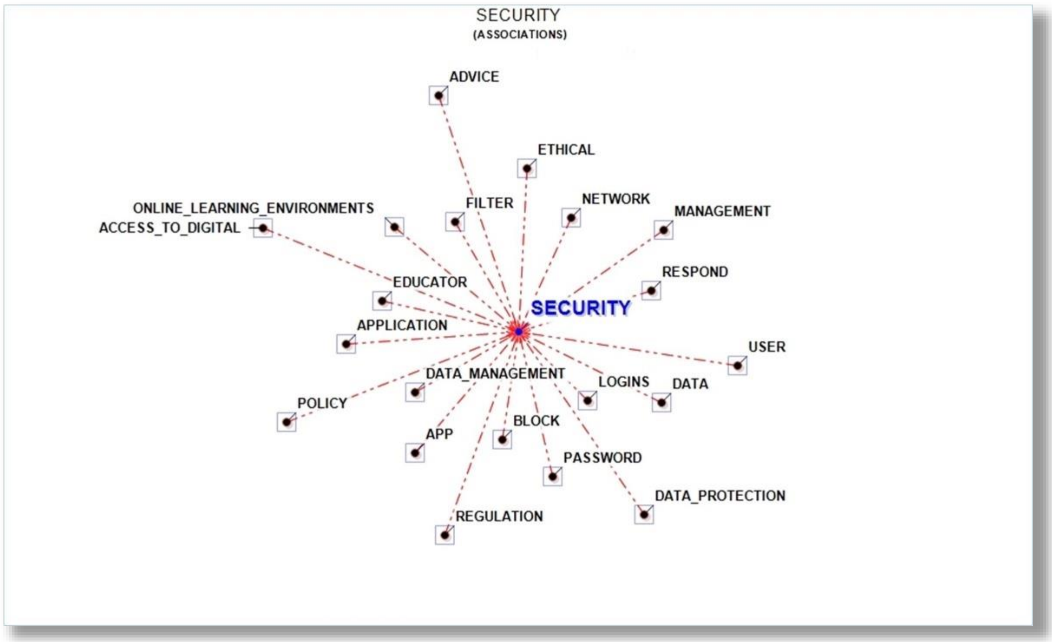


Fig. 13 – Focus on the lemma "SECURITY" with word associations

The above key words (labels with frequency ≥ 4) that are significantly associated with the word "security" ($p \leq 0.05$) within the text corpus and the related $\chi 2$ value are as follows: (logins - 34.46), (block - 23.17), (data_management - 23.17), (educator - 18.40), (filter - 18.40), (network - 18.40), (respond - 18.40), (data - 9.76), (password - 10.24), (app - 11.12), (application - 11.12), (online_learning_environments - 11.12), (ethical - 9.05), (management - 9.05), (user - 5.38), (data_protection - 5.48), (regulation - 5.48).

5.2 Description/reification of competences in the digital education & cybersecurity fields

Irrespective of the structural dimension of the surveyed **EC digital competence frameworks and self-assessment tools** (namely how they organise, group, classify and/or categorise digital competences, including those concerning cybersecurity), at 'leaf-level' they mostly reify individual competences by way of a title plus brief descriptive text, commonly referred to as a "descriptor" or - more simply - "item". This is usually coupled with - or in the form of - a specific action statement ("I **foster** …., I **develop** …., "In our school we **learn** …..") or capacity ("**I can** identify …..") . Exceptions to such 'action-oriented' descriptors are found in two cases:

- the DigCompOrg framework (JRC, 2015), which pairs a generalised statement (e.g. "*Safety, risks and responsible behaviour in online environments are foregrounded*") with a brief definition (e.g. "*Staff and student digital competence comprehensively addresses*….")
- The European Cybersecurity Skills Framework (EC-ENISA, 2022), which defines professional cybersecurity profiles, including "Cybersecurity Educator", by listing – among other attributes – the **main tasks** ("*Develop, update and deliver cybersecurity and data protection curricula* ……") and **key skills** ("*Design, develop and deliver learning programmes"*) typifying each profile.

It is worth noting here that the **DigComp 2.2 Framework** not only defines the digital competences themselves, it also provides comprehensive listings of **Knowledge, Skills and Attitudes** associated with each competence, together with (proficiency-graded) **Use Cases** in professional and education domains, respectively.

The mission of the other documents surveyed here, namely the **blended learning guidelines and handbook** and the **bullying-in-schools factsheet,** differs distinctly from the others. Rather than framing/describing digital competences/capacities in education generally , they provide recommendations for various education stakeholders on how to meet the challenges at hand, including best practices to follow. That said, "**Blended learning in school education – guidelines for the start of the academic year 2020-2022**" (EC, 2020) does provide a structured framework of key considerations for "successful blending learning". This comprises eight thematic areas, each grouping a set of sub-considerations potentially transformable into "guiding questions for stakeholders, for example: "Does our system have in place…?" or "How can our schools…?". What's more, "**Blended learning for high quality and inclusive primary and secondary education – Handbook**" (EC, 2021) includes a broad overview of a number of the EC documents and tools surveyed here. It also advocates adoption of legal frameworks to support appropriate and effective decision making by "governing authorities (local authorities, school board, school leadership team)", something which could involve "adapting Initial Teacher Education and teacher competence frameworks, if appropriate" (p.12).

5.3. Competence Proficiency Positioning & Grading

Beyond defining digital competences in education, the **surveyed EC digital competence frameworks and self-assessment tools** also set these competences on progressive proficiency scales (all except DigCompOrg, which – as mentioned – describes competences in conceptual/descriptive terms rather than in the form of 'action statement' items). Adoption of proficiency scales not only helps more accurate positioning of users'/respondents' actual competence levels at any given time, it also provides a structured vision and conceptual scaffolding for scaling up those levels.

Competency items in **DigComp 2.2** are ranked according to eight-level proficiency scales, while **DigCompOrg** and **SELFIEforTeachers** adopt a comprehensive competency proficiency model with six levels. In all these cases, however, the various 'action statement' items ("I can…", "I develop….") that encapsulate individual competences are graded to reflect progression in competency development/complexity. The grading of the respective competence item-statements not only reflects progressive domain content-related specialisation and/or expertise, it also draws evident inspiration from the learning taxonomy proposed by Bloom (1956) - and later revised by Anderson & Krathwohl (2001) - i.e. progressing through the stages from passive knowledge/awareness to more proactive creation and evaluation.

DigComp 2.2 adopts a structured proficiency scale that has four macro levels (Foundation, Intermediate, Advanced, Highly Specialised), each of which covers two proficiency levels (1-2, 3-4, 5-6, 7-8 respectively). In addition, at each level the related "I can …" statements themselves are framed and worded progressively, as shown in Table 2 below.

Table 2 *- structured proficiency scale adopted in DigComp 2.2*

PROFICENCY LEVEL	PROGESSIVE FRAMING OF CORRESPONDING "I CAN …" STATEMENTS
• Foundation level 1	*At basic level and with guidance, I can …*
• Foundation level 2	*At basic level and with autonomy and appropriate guidance where needed, I can …*
• Intermediate level 3	*On my own and solving straightforward problems, I can …*
• Intermediate level 4	*Independently, according to my own needs, & solving well-defined, non-routine problems, I can …*
• Advanced level 5	*As well as guiding others, I can …*
• Advanced level 6	*At advanced level, according to my own needs and those of others, and in complex contexts, I can*
• Highly Specialised level 7	*At highly specialised level, I can …*
• Highly Specialised level 8	*At the most advanced and specialised level, I can …*

The **DigCompEdu** framework and **SELFIEforTeachers** self-assessment tool based on that framework both adopt the comprehensive, highly structured **DigCompEdu Progression Mode**l (fig.5). This conceptual model provides the basis for the DigCompEdu graded proficiency levels (fig. 6 plus summarised version in fig. 13 below), which progressively rank the presented competences. A particularity of this proficiency ranking is that it is expressed in terms of six functional profiles, ranging from "Newcomer" though to "Pioneer" (see below).

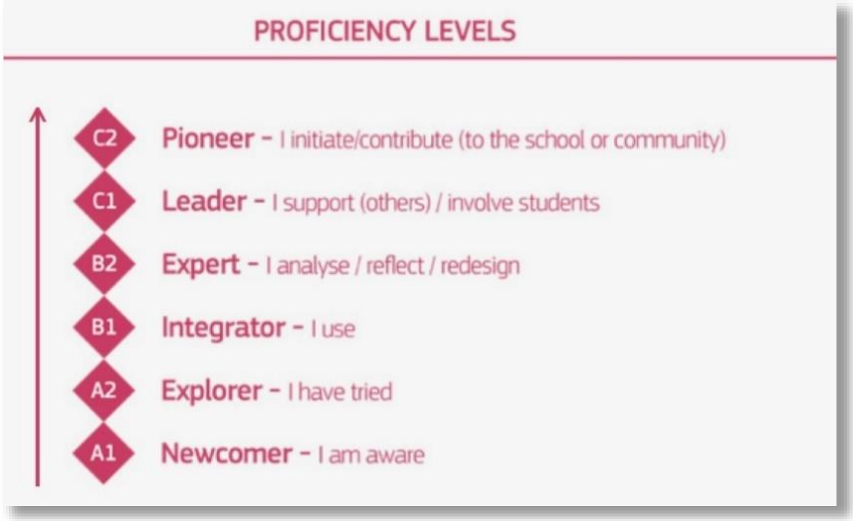

PROFICIENCY LEVELS
C2
Pioneer - I initiate/contribute (to the school or community)
C1
Leader - I support (others) / involve students
B2
Expert - I analyse / reflect / redesign
B1
Integrator - I use
A2
Explorer - I have tried
A1
Newcomer - I am aware

Fig. 13 - SELFIEforTEACHERS proficiency levels based on theDigCompEdu Progression Model [22]

As the figure above shows, each of these profiles is correlated to the consolidated codification system [A1 – A2 – B1 – B2 – C1 – C2] introduced in the **Common European Framework of Reference for Languages – CEFR** (Council of Europe, 2020, 2001). This ground-breaking European competency framework, developed and published by the Council of Europe, is now pervasive in educational, academic and professional spheres throughout Europe and beyond. The choice to adopt the CEFR competency level codification lends the DigCompEdu Progression Model familiarity to DigCompEdu and SELFIEforTeachers users, as does the reification of competencies in action-based "I can ...." statements, another key characteristic of the CEFR approach. DigCompEdu/SELFIEforTeachers proficiency levels.

5.4 SuperCyberKids Skills Framework (SCKSF) & EC digital competence initiatives: opportunities

[22] Figure from Economou, A., SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

As mentioned at the beginning of this document, development of cybersecurity competences in the educational sphere is inexorably entwined with support for the furthering of digital competences generally within education at different levels. Hence efforts on both these fronts can yield synergies and mutual benefits that potentially boost efforts to attain the goals of the EC's Digital Education Action Plan 2021-2027, or DEAP (European Commission, 2020).

Firstly, the analysis of EC digital competence frameworks and self-assessment tools reported here (just like the other preparatory studies performed in SCK Work Package 2) is intended to help ground, inform and orientate drafting of the "SuperCyberKids Skills Framework" (SCKSF), lending the SCKSF a firmer conceptual basis. Synergic alignment between SCKSF and the surveyed initiatives could also be beneficial, at both conceptual and operative levels.

Secondly, SCKSF could provide useful input on cybersecurity matters and issues for consideration as part of existing EC endeavours to develop digital competences in education: for example, SCKSF may yield content that could ultimately be considered for incorporation to some degree in updated versions of the EC frameworks and self-assessment tools surveyed here. But in the meantime, one very tangible opportunity for cross-fertilisation stands out. **Recommendations on cybersecurity education in schools generated in the SCK project could be formulated as a proposed set of optional SELFIE items that schools' SELFIE Coordination Teams can draw on for possible inclusion in their SELFIE questionnaires**. A parallel example of such domain-specific SELFIE ecosystem enrichment already exists, namely "Suggested optional SELFIE questions on blended learning"[23], a resource currently available on the EC SELFIE portal[24]. Obviously, **formulation of SCK-derived cybersecurity recommendations in typical SELFIE-item structure and format would constitute merely a first step in the process: such items would need to undergo appropriate validation, pilot testing and translation/localisation before ultimate publication as proposed optional SELFIE items**.

[23] https://education.ec.europa.eu/sites/default/files/document-library-docs/blended-learning-nov21_en.pdf

[24] https://education.ec.europa.eu/selfie/resources#pubs

6. REFERENCES

Anderson, L. W. & Krathwohl, D. R. (2001). A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. New York: Longman.

Bloom, B.S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain.

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use, EUR 28558 EN, doi:10.2760/38842

Council of Europe (2020), Common European Framework of Reference for Languages: Learning, teaching, assessment – Companion volume, Council of Europe Publishing, Strasbourg. Retrieved 07-06-2023 at: https://www.coe.int/en/web/common-european-framework-reference-languages

Council of Europe (2001) Cambridge University Press. A Common European Framework of reference for Languages: Learning, teaching, assessment. Cambridge University Press. Retrieved 07-06-2023 at: http://assets.cambridge.org/052180/3136/sample/0521803136ws.pdf

Economou, A., (2023). SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

EPRS - European Parliamentary Research Service, Binder K., (2023). "Progress on the European Commission's 2021-2027 digital education action plan". European Parliament Briefing paper PE 745.689 – March 2023. © European Union. Retrieved 05-06-2023 at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)745689

European Commission (2022). Discover the Digital Potential of Your School – SELFIE Questionnaires (EN). Retrieved 07-06-2023 at https://education.ec.europa.eu/sites/default/files/2022-07/SELFIE_Questionnaires_EN.pdf

European Commission (2021). SELFIE Guide for School Coordinators. Retrieved 07-06-2023 at https://education.ec.europa.eu/document/setting-up-selfie-in-your-school-detailed-guide-for-selfie-school-coordinators

European Commission, Directorate-General for Education, Youth, Sport and Culture, (2023). *What can schools do about bullying?*, Publications Office of the European Union, , https://data.europa.eu/doi/10.2766/809742

European Commission, Directorate-General for Education, Youth, Sport and Culture, (2021). Blended learning for high quality and inclusive primary and secondary education – Handbook, Publications Office of the European Union, https://data.europa.eu/doi/10.2766/237842

European Commission, (2020). Digital Education Action Plan 2021-2027: Resetting education and training for the digital age. Retrieved 05-06-2023 at https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624

European Commission, Directorate-General Education, Youth, Sport and Culture, Unit B.2: Schools and multilingualism (2020). Blended learning in school education – guidelines for the start of the academic year 2020/21. Retrieved 07-06-2023 at: https://www.schooleducationgateway.eu/downloads/Blended%20learning%20in%20school%20education_European%20Commission_June%202020.pdf

European Commission, Joint Research Centre, Punie, Y., Pujol Priego, L., Carretero, S. et al., (2018). DigComp into action, get inspired make it happen – A user guide to the European Digital Competence framework, Punie, Y. (editor), Carretero, S. (editor), Vuorikari, R. (editor), Publications Office, https://data.europa.eu/doi/10.2760/112945

European Union Agency for Cybersecurity, ECSF, (2022). European cybersecurity skills framework, https://data.europa.eu/doi/10.2824/859537

European Union Agency for Cybersecurity (ENISA), (2022). User Manual, ECSF - European Cybersecurity Skills Framework. ISBN: 978-92-9204-583-8 – DOI: 10.2824/95989

Joint Research Centre, Institute for Prospective Technological Studies, Devine, J., Punie, Y., Kampylis, (2015). Promoting effective digital-age learning – A European framework for digitally-competent educational organisations, Publications Office, https://dx.doi.org/10.2791/54070

Lancia, F. (2012). T-lab Pathways to Thematic Analysis. Retrieved 15-06.2023 at: https://mytlab.com/tpathways.pdf

Redecker, C. (2017). European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, , ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

Vuorikari, R., Kluzer, S. and Punie, Y., (2022). DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415