



# **Guidelines targeting schools for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) - final version.**

## **SuperCyberKids Deliverable no D6.1**

Call: ERASMUS-EDU-2022-PI-FORWARD

Type: R - Document

Project No. 101087250



**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 the granting authority can be held responsible for them.

<b>Project ref. number</b>	101087250
<b>Project title</b>	<b>SCK - SuperCyberKids</b>
<b>Document title</b>	Guidelines targeting schools for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) - final version.
<b>Document Type</b>	R-Document
<b>Document version</b>	V1 – 14/10/2025
<b>Previous version(s)</b>	/
<b>Language</b>	English
<b>Planned date of delivery</b>	30.11.2025
<b>Dissemination level</b>	Public
<b>Number of pages</b>	28
<b>Partner responsible</b>	EC SO
<b>Author(s)</b>	Anne-Sophie Van Vaerenbergh – European Cyber Security Organisation
<b>With contributions by:</b>	All partners
<b>Keywords</b>	Game-based learning, Cybersecurity Education; Guidelines
<b>DOI</b>	<a href="https://doi.org/10.17471/54035">https://doi.org/10.17471/54035</a>
<b>How to cite</b>	Van Vaerenbergh. A. S. (2025). Guidelines targeting schools for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) - final version. Deliverable 6.1 - SuperCyberKids project (ERASMUS-EDU-2022-PIFORWARD - ERASMUS-LS - Project No. 101087250). DOI: <a href="https://doi.org/10.17471/54035">https://doi.org/10.17471/54035</a>

# Internal project peer review process

Approved by		
Manuel Gentile	Project Coordinator (CNR-ITD)	28/11/2025

# Table of Content

1	Introduction	5
2	Working Package 6	5
2.1	Overview of documents of Working Package 6	5
3	Real Guidelines	6
3.1	Introduction to the SuperCyberKids Project	6
3.2	General introduction to Cybersecurity Education	7
3.2.1	Cybersecurity for kids, why should we care?	7
3.2.2	Why might children be target? And why should schools care?	7
3.2.3	The Need for a Unified EU Framework	8
3.3	The SuperCyberKids Learning Framework	8
3.3.1	Development of a competency framework	8
3.3.2	Summary of the Pillars	9
3.3.3	Literature Review – Key Findings	9
3.3.4	Initiative Survey – Key Findings	9
3.3.5	Framework Analysis	10
3.4	The SCK Learning Framework Competencies Explorer	10
3.4.1	Competencies	10
3.4.2	Ontology	10
3.4.3	Formalising the concept of competence in an ontology	11
3.4.4	The SuperCyberKids Learning Framework Ontology	11
3.4.5	The SCLF Ontology: one of the instances sub-domains	11
3.4.6	A tool to explore the SCKLF Ontology	12
3.4.7	Smart search functionality	12
3.4.8	Relevance Index	12
3.4.9	Exploring the results	13
3.4.9.1	Minimum set	13
3.4.9.2	Inspecting the details of the elements	13
3.4.9.3	Step-by-step exploration	13
3.5	The Curriculum	14
3.5.1	Lessons Plans for 7 out of the 18 modules	14
3.5.2	Details about the 7 modules that contain a lesson plan	15
3.5.3	Game Based Approach	16
3.6	The Platform	17



3.6.1	Platform Landing Page	17
3.6.2	How to register (standard use)	17
3.6.3	How to register for the SuperCyberKids Pilot testing (invitation only)	17
3.6.4	Log in to the platform	17
3.6.5	The Platform's Home Page	18
3.6.6	The Navigation Menu	18
3.6.7	Platform Items	19
3.6.8	A SuperCyberKids Module	19
3.6.9	Feedback form	20
3.6.10	Community Items	20
3.6.11	Search Function	20
3.6.12	Add item to the Community	21
3.6.13	Add item to share it with the Community	21
3.6.14	Add item to playlist	22
3.6.15	Select pr create a playlist	22
3.6.16	View items you have uploaded	22
3.6.17	View your profile	23
3.7	Assessment of Student Achievement	23
3.7.1	Knowledge test about Cybersecurity	23
3.8	Modules	25
3.9	Next Steps for participating in the Pilot Phase	25
4	Appendix	25
4.1	General Powerpoints	25
4.2	Powerpoints of each pilot	26
4.3	Lessonsplans of each module	27

# 1 Introduction

SuperCyberKids (SCK) is a European project that promotes cybersecurity awareness and digital literacy among schoolchildren aged 8 to 13 through a game-based learning ecosystem. It provides age-appropriate, interactive tools to help educators teach key cybersecurity concepts in engaging and accessible ways.

This document presents an overview of the guidelines aimed at supporting schools, particularly head teachers and teachers, in integrating a game-based learning ecosystem on cybersecurity into the curriculum for schoolchildren aged 8 to 13. These guidelines are part of a broader European initiative to foster cybersecurity awareness and digital resilience among young learners.

## 2 Working Package 6

Work Package 6 (WP6) was instrumental in operationalising the project's core objectives by translating the conceptual framework into real-world educational settings. It directly addressed three key objectives of the project: promoting teacher professional development on cybersecurity (Ob.2.a), designing and implementing localised pilot use cases across Europe (Ob.2.c), and producing actionable guidelines for integrating the digital ecosystem into school curricula (Ob.3.b). WP6 coordinated the implementation of four distinct pilot use cases, in Italy, Estonia, Germany, and an EU-based context, each adapted to local educational systems and cultural contexts. These pilots were preceded by targeted online teacher training initiatives and followed by classroom experimentation using co-designed learning activities. The diversity of the pilot environments allowed the project to test the flexibility, relevance, and impact of the ecosystem across different educational landscapes.

### 2.1 Overview of documents of Working Package 6

- Document D6.1 'Guidelines targeting schools for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) - final version.' - [SCK-D6.1 \(version 1\).docx](#) (This Document).
- Excel tracker for the pilot leads to keep track of the numbers and an overview of all teachers participating in the pilot. - [SuperCyberKids Tracking Teacher Training & Pilot Phase.xlsx](#)
- Pilot Report ([SCK - Pilot Report.docx](#)) giving a full overview (aligned with the excel tracker & the proof provided in the maps), around:
  - T6.2 : Piloting of the ecosystem on cybersecurity education in ITALY
  - T6.3 : Piloting of the ecosystem on cybersecurity education in ESTONIA
  - T6.4 : Piloting of the ecosystem on cybersecurity education in GERMANY
  - T6.5 : Piloting of the ecosystem on cybersecurity education - EU-BASED IN ENGLISH LANGUAGE
- Feedback is collected via questionnaires (pre and post questionnaire for the teacher training and post questionnaire for the pilot phase). Beside the questionnaires, we have also provided proof of all teacher trainings & pilots happening in each pilot phase which can be found in the following map: [WP6 - Proof of Teacher Training & Pilot Phase](#). Important to highlight is that the evaluation of both teacher training initiatives and pilot use cases will be carried out in Working Package 7 with the lead beneficiary being Avanzi (Erica Melloni).

### 3 Real Guidelines

All guidelines are captured in PowerPoints via: CNR-ITD\SuperCyberKids - WP6 - Implementation of pilot use cases in schools\PPTs for teacher training

WP6 - Implementation of pilot use cases in schools				
WP6 - Implementation of pilot use cases in schools > PPTs for teacher training				
Name	Modified	Modified By	Add column	
[NL] Translation	February 26	Petra van Haren		
01_General introduction to CyberSecurityEducation.pptx	January 7	Manuel Gentile		
02_The SuperCyber Kids Learning Framework.pptx	February 10	Anne-Sophie Van Vae		
03_The SCKLF Competencies Explorer.pptx	February 10	Anne-Sophie Van Vae		
04_SuperCyberKids pilot ppt draft_split.pptx	February 10	Anne-Sophie Van Vae		
05_The Assessment of the Student's Achievements (1).pptx	March 3	r.memeo		
06_SuperCyberKids platform training_v1.pptx	April 4	Jeffrey Earp		
07_TT Intro Modules_1_2_3_4_v1.pptx	April 7	Nicolai Plintz		
08_TT Intro Modules_5_6_7_v1.pptx	January 27	peadarcallaghan		
SCK_PPTX_Template.pptx	December 15, 2023	Manuel Gentile		
Summary guidelines for teachers_v1.pptx	April 4	Jeffrey Earp		

Below a short overview of these PowerPoints.

#### 3.1 Introduction to the SuperCyberKids Project

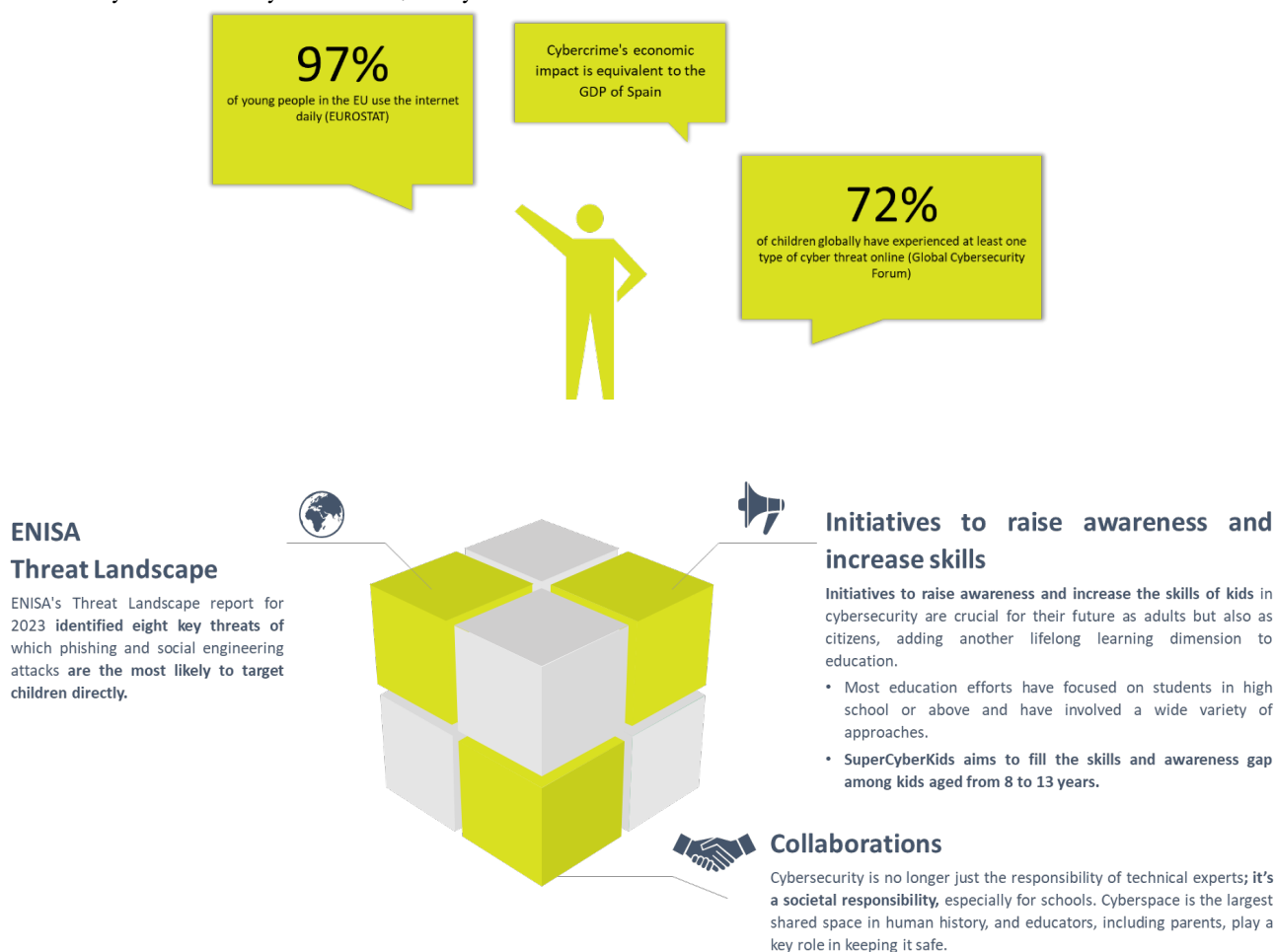
SuperCyberKids project is developed in partnership with the European Commission (Erasmus+ Programme) and the European Schools Head Association (ESHA). It's to raise awareness around cybersecurity for schoolchildren aged 8 to 13.

The SuperCyberKids platform is a free, gamified educational tool that provides interactive cybersecurity games and resources for children, along with customizable content management for teachers to enhance the learning experience.

The pilot phase will be conducted in Italy, Germany, Estonia, and selected EU-based English-speaking schools from February to November 2025. Following this period, participation in the pilot will be possible.

## 3.2 General introduction to Cybersecurity Education

### 3.2.1 Cybersecurity for kids, why should we care?



### 3.2.2 Why might children be target? And why should schools care?

- Children are often targeted through shared family devices, which can accidentally download malware.
- Poor habits like reusing passwords increase the risk, and children may unknowingly share personal information or access sensitive details like credit cards, making them vulnerable to phishing or blackmail.
- Cybercriminals use phishing to access children's gaming accounts and steal or sell virtual items. All accounts are at risk, even if they don't have valuable items, as hackers target them indiscriminately.
- While high-level ransomware attacks typically target organizations, children may be vulnerable to ransomware in online games, where their virtual property can be stolen or held for ransom. Students should be aware of this risk and practice good cyber hygiene.
- Children are increasingly targeted by online activities that aren't illegal but can still cause harm. Microtransactions in free games encourage spending small amounts of money, often without realizing the total cost.

- Loot boxes, a form of in-game gambling, are also rising, where players may win valuable items or nothing at all. Both issues highlight the need for cyber hygiene education to help children understand these risks.
- Cyber education must raise awareness of dangers without encouraging children to experiment with harmful tools, similar to how drug education informs without promoting use.
- Some believe children can't be effective hackers, but this is false. Beginner hackers, or "script kiddies," use online code to cause damage without fully understanding it. Basic coding skills, like installing mods or following instructions, can enable these attacks.
- Cybersecurity education should teach both defense and ethical guidelines, helping kids understand legal boundaries and redirecting their curiosity toward positive cybersecurity pursuits.
- Cybersecurity education for children aged 8-13 is becoming increasingly important due to the growing complexity of digital threats. Integrating cybersecurity topics into existing subjects like IT, Computer Science, and General Studies ensures students learn key concepts without overhauling the curriculum. Additionally, accessible online resources, such as courses and games, extend learning beyond the classroom, catering to diverse student needs.

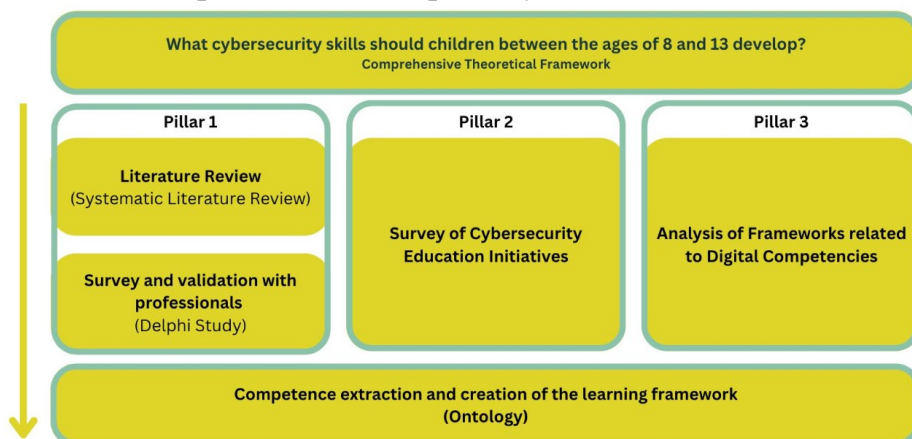
### 3.2.3 The Need for a Unified EU Framework

The introduction of Cybersecurity Education for children aged 8-13 requires a standardised EU framework, like the SuperCyberKids project, which integrates game-based learning into existing curricula with guidelines for educators. Key benefits include:

- **Consistency Across Member States:** Ensures a unified approach to cybersecurity education across the EU.
- **Pedagogical Efficacy:** Game-based learning enhances engagement and skill transfer but requires sound pedagogical guidance.
- **Ethical and Legal Considerations:** Sets boundaries to ensure ethical teaching and prevent misuse.
- **Self-regulated Learning:** Encourages students to manage their learning in an ever-changing cybersecurity landscape.
- **Quality Assurance:** Guarantees alignment of learning outcomes with educational standards.
- **Facilitation of Teacher Training:** Supports teacher development to effectively teach cybersecurity.

## 3.3 The SuperCyberKids Learning Framework

### 3.3.1 Development of a competency framework



3.3.2 Summary of the Pillars

Literature Review	Initiative Survey	Framework Analysis
<ul style="list-style-type: none"><li>• Systematic Literature Review</li><li>• Identified over 500 necessary skills</li><li>• Validation of skills by experts</li></ul>	<ul style="list-style-type: none"><li>• 65 existing programs analyzed</li><li>• Best practices identified</li><li>• Success factors evaluated</li></ul>	<ul style="list-style-type: none"><li>• EC digital competence frameworks</li><li>• Self-assessment tools</li><li>• Educational guidelines</li></ul>

As part of the foundational research for the SuperCyberKids project, a Comprehensive Theoretical Framework was developed to identify the cybersecurity skills children aged 8 to 13 should acquire. This process led to the extraction of over 500 relevant skills, which were systematically organized into the SuperCyberKids Learning Framework Ontology (SCKLF-Ontology). The ontology serves as a structured model that categorizes and connects competencies within the field of cybersecurity.

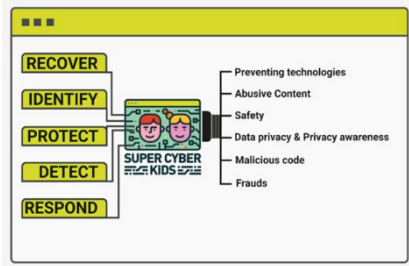
It includes a:

- **Skills taxonomy:** identification of relevant skills (e.g. data protection, fraud prevention).
- **Cybersecurity domains:** areas such as malicious code, data security, fraud prevention.
- **Categories and relationships:** linking skills to learning outcomes and game-based activities.

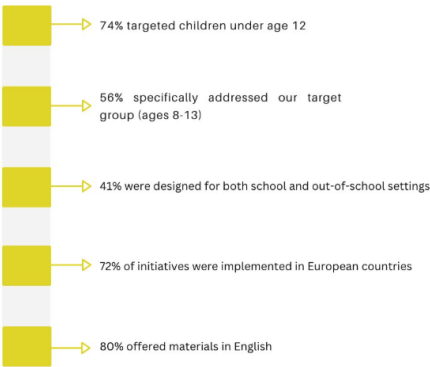
This framework ensures that the educational content is both pedagogically sound and aligned with real-world cybersecurity challenges.

3.3.3 Literature Review – Key Findings

- Over 500 relevant skills were extracted from the literature and the Delphi study
- Validation via 2-Round Delphi Study with 20 Professionals
- Matrix-based Approach
- Literature review with six leading databases (Prisma)



3.3.4 Initiative Survey – Key Findings



- In our comprehensive survey, we examined initiatives across Europe and beyond, analyzing their approach to cybersecurity education.
- Each initiative was systematically coded using a structured survey form covering four key areas:
  - Description of the initiative/program
  - Competency domains addressed
  - Learning path and curriculum design
  - Additional observations and context

### 3.3.5 Framework Analysis

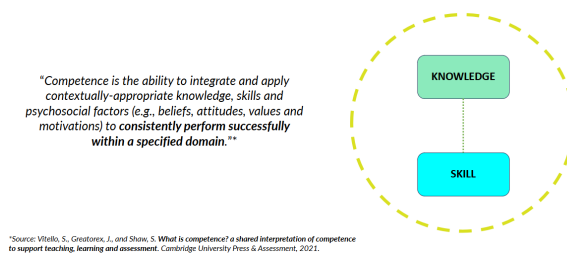
The pillar is based on nine EC initiatives, including for example:

- DigComp 2.2 (digital citizenship skills framework)
- DigCompEdu (framework for teachers)
- SELFIE (self-assessment tool for schools)
- ECSF (European Cybersecurity Skills Framework)
- Guidelines on blended learning and cybersecurity aspects were also taken into account.

## 3.4 The SCK Learning Framework Competencies Explorer

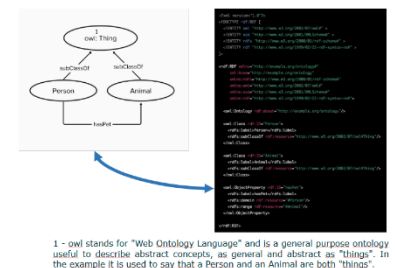
### 3.4.1 Competencies

- Many different definitions used for the concept
- There is also linguistic confusion (Competency? Competence?)
  - Often times it depends on the context: Behavioural vs Task-oriented; USA vs UK;
- In almost all of the definitions Competence is formalised as a holistic concept
  - It is important to consider each part of the macro-concept of Competence to fully understand it
- This topic is addressed in more depth in the SCK Learning Framework, but in this context it is important to be mindful of the nature of the concept of competence

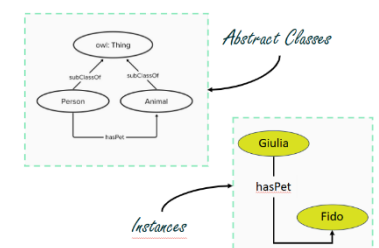


### 3.4.2 Ontology

- An ontology is a structured representation of a knowledge domain.
- It is a formalism that is useful to clearly and more easily understand topics, but importantly it is also suitable for machine processing (e.g. Semantic Web).
- By virtue of their formal structure, ontologies have the benefit of being easy to share. This makes it possible to create large dictionaries, reuse concept descriptions, and in general disambiguate knowledge.



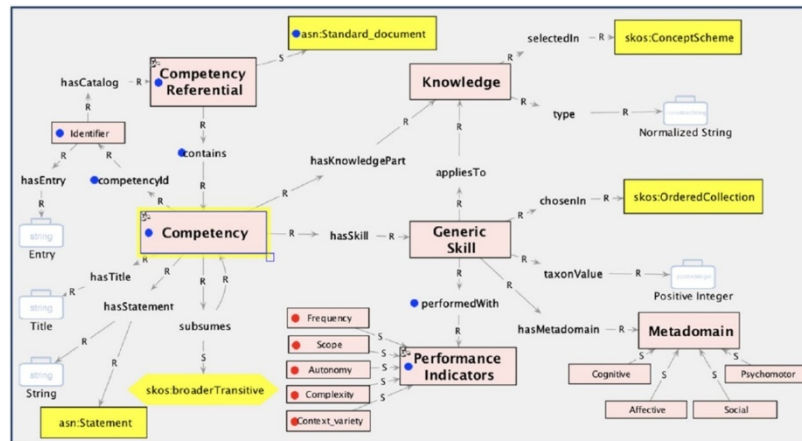
- An ontology defines concepts as classes:
  - the abstract representation of a category of elements
- Each ontology class can have concrete instances. For examples, "Giulia" is a concrete instance of the abstract class "Person"
- Classes and instances can be related to other elements through the use of relationships





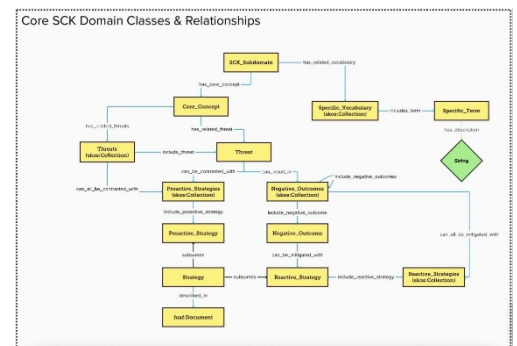
### 3.4.3 Formalising the concept of competence in an ontology

- In SuperCyberKids, to describe the concept of competence and its parts, we use an ontology already available in the literature: COMP2
- You can think of COMP2 as a vocabulary we use in order to be unambiguous and share a common representation of competence.
- As seen before, COMP2 describes a competency as being composed of some knowledge and some generic skill that is applied to it.

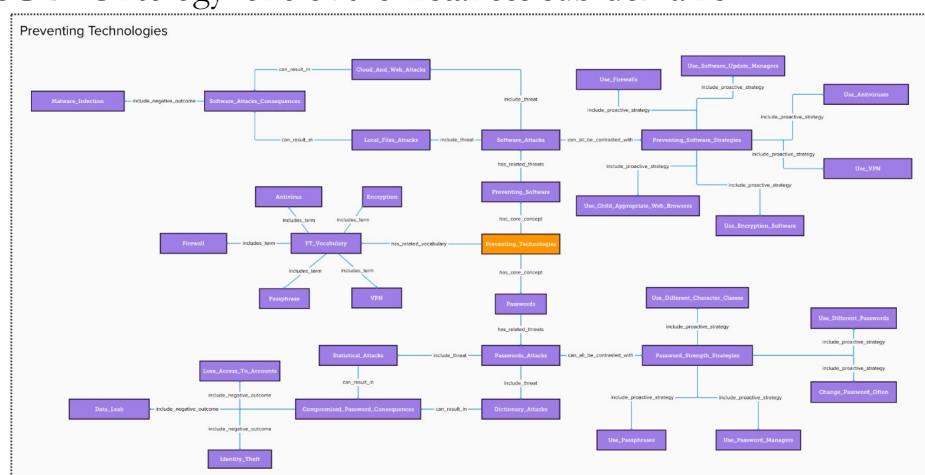


#### 3.4.4 The SuperCyberKids Learning Framework Ontology

- For the description of the knowledge domains referenced by the competences, we created a new ontology.
- This ontology allows us to clearly and unambiguously define (i) the various classes of knowledge elements that we need to describe the various domains concerned, and (ii) the instances of concrete elements linked to them
- These abstract classes define the sub-domains, the key concepts of each sub-domain, the vocabulary used, the main threats together with the strategies (both proactive and reactive) used to prevent and mitigate the related negative outcomes



### 3.4.5 The SCLF Ontology: one of the instances sub-domains





### 3.4.6 A tool to explore the SCKLF Ontology

- As can be seen in the previous example, these knowledge formalisations can expand very quickly and become difficult to navigate, even when expressed in graphic form.
- This is why we have created a tool that allows the identification of skills related to a particular topic (or a particular keyword), helping the user in a smooth and gradual exploration of this knowledge space identified within the ontology.
- As can be seen in the previous example, these knowledge formalisations can expand very quickly and become difficult to navigate, even when expressed in graphic form.
- This is why we have created a tool that allows the identification of skills related to a particular topic (or a particular keyword), helping the user in a smooth and gradual exploration of this knowledge space identified within the ontology.
- Although the tool automatically displays an optimal visualisation of the retrieved information, you can freely reposition any element within the graph as desired.



### 3.4.7 Smart search functionality

- Competencies are found by using the smart search functionality, using topics and key terms
- The system will collect results based on the information contained in the ontology
- Competencies shown in the results list will be closely related to the search topics or terms used (even if the term is not present in the competency definition itself)

Use Strategies To Protect Against And Prevent Cyberbullying [Relevance Index: 8]	▼
Develop And Implement The Correct Actions In Cases Of Cyberbullying [Relevance Index: 4]	▼
Detect And Identify Online Risks And Threats That Need The Assistance Of An Adult And Ask For Help [Relevance Index: 2]	▼
Understand Online Etiquette And Behaviour [Relevance Index: 2]	▼

### 3.4.8 Relevance Index

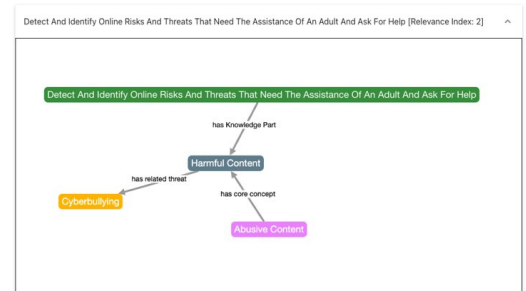
- Each competence shown in the results is accompanied and described by a relevance index
- This index shows how closely related a competence is to the term or topic used in the search

Use Strategies To Protect Against And Prevent Cyberbullying [Relevance Index: 8]	▼
Develop And Implement The Correct Actions In Cases Of Cyberbullying [Relevance Index: 4]	▼
Detect And Identify Online Risks And Threats That Need The Assistance Of An Adult And Ask For Help [Relevance Index: 2]	▼
Understand Online Etiquette And Behaviour [Relevance Index: 2]	▼

### 3.4.9 Exploring the results

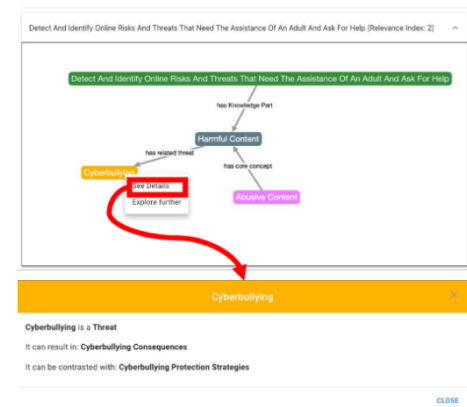
#### 3.4.9.1 Minimum set

- By clicking on each result, the system will display the minimum set of elements characterising the competence in question
- This set of elements is displayed by the system in the form of an oriented graph, making it easier to understand both the elements and the relationships between them
- This first set of elements allows the user to contextualise the result, see the link with the topic entered in the search bar, and begin to explore the concepts most closely related to the competence
- Each of the elements contained in the minimum set can be analysed by displaying the details. Similarly, each element can be used for a step-by-step exploration.



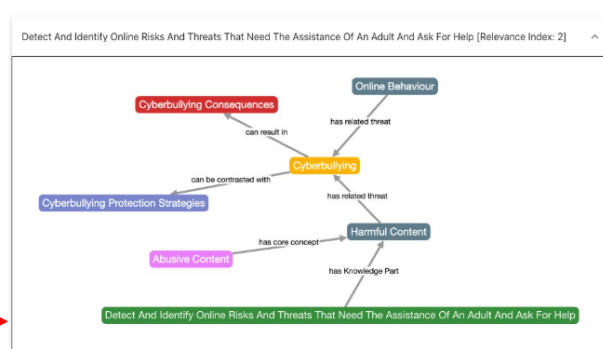
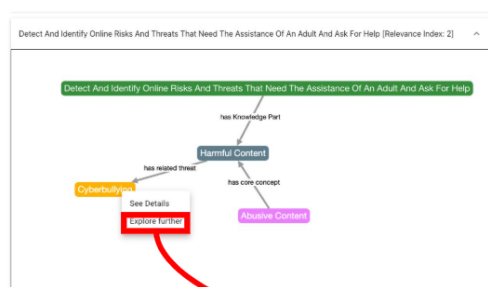
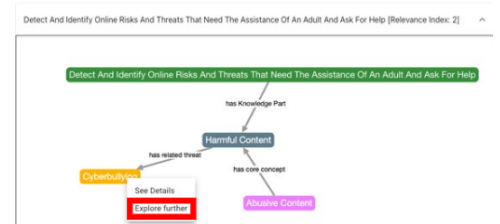
#### 3.4.9.2 Inspecting the details of the elements

- By right-clicking on any displayed element, a contextual menu will allow you to choose whether to view details of the element or use it as a basis for further exploration of concepts.
- The detailed view (bottom) displays all direct information that characterises the element within the ontology
- Words in this view that represent key terms within the ontology are highlighted in bold



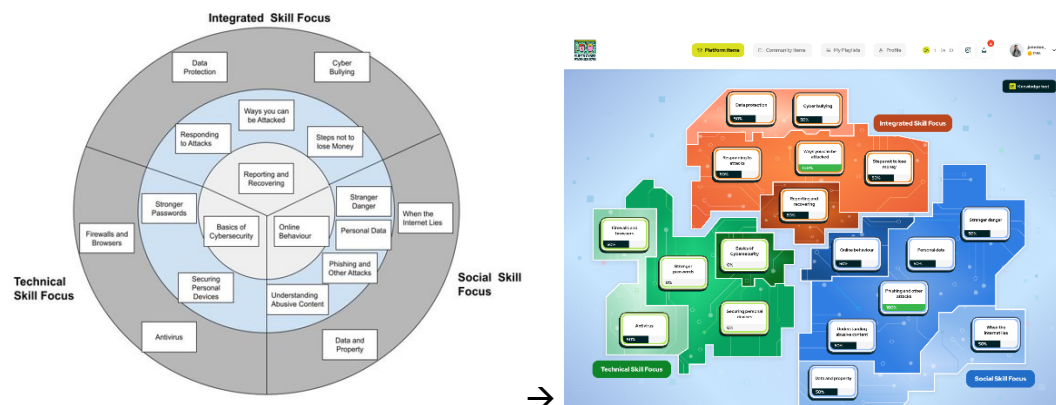
#### 3.4.9.3 Step-by-step exploration

- Alternatively, clicking on 'Explore further' will expand the graph with new elements and concepts related to the selected item
- This allows guided, step-by-step exploration of the complex network of information contained within the ontology
- This way you can explore only the portions of information that you consider relevant and useful, while minimising unnecessary clutter.
- To facilitate visualisation, the system will also automatically reconfigure the arrangement of elements within the graph.



## 3.5 The Curriculum

Building on the SuperCyberKids Learning Framework, 18 educational modules were developed to support the teaching of cybersecurity concepts to children aged 8 to 13. These modules are thematically organized into three core fields: Technical, focusing on foundational digital and cybersecurity skills; Social, addressing responsible online behavior and digital citizenship; and Integrated, combining technical and social elements to reflect real-world scenarios. This structure ensures a balanced and comprehensive approach to cybersecurity education, tailored to the developmental needs of young learners.



### 3.5.1 Lessons Plans for 7 out of the 18 modules

Lesson plans have been developed for 7 out of the 18 modules in the cyber security curriculum. These include:

- Module 1: Basics of Cyber Security
- Module 2: Online Behaviour
- Module 3: Reporting and Recovery
- Module 4: When the Internet Lies
- Module 5: Stronger Passwords
- Module 6: Understanding Abusive Content
- Module 7: Cyber Bullying

Each module includes detailed classroom activities designed to help teachers raise awareness, encourage safe online behavior, and equip learners with the skills to navigate digital environments confidently and responsibly. Each module is structured into four lesson plans: Introduction, Game-Based Learning, Consolidation, and Assessment & Feedback. Each lesson is designed to last approximately one hour, making the total duration to complete a module around four hours. All lesson plans are available on the SuperCyberKids platform (See example lesson plan in Annex).

Lesson Plan 1 - Intro				
Activity	Time	Details	Learning Goal	Notes
1. Welcome and Introduction	10 min	Teacher introduces the module and its objectives. Students share their expectations for the module.	Students understand the module's goals and objectives.	
2. Basics of Cyber Security	15 min	Teacher explains the basics of cyber security, including the importance of keeping personal information safe and the risks of sharing information online.	Students understand the basics of cyber security and the importance of keeping personal information safe.	
3. Online Behaviour	15 min	Teacher discusses online behavior, including the importance of being respectful and responsible online, and the risks of cyberbullying.	Students understand the importance of being respectful and responsible online, and the risks of cyberbullying.	
4. Reporting and Recovery	15 min	Teacher explains the importance of reporting cyber incidents and the steps to take if a cyber incident occurs.	Students understand the importance of reporting cyber incidents and the steps to take if a cyber incident occurs.	
5. When the Internet Lies	15 min	Teacher discusses the risks of phishing and other online scams, and the importance of being cautious when clicking on links or downloading files.	Students understand the risks of phishing and other online scams, and the importance of being cautious when clicking on links or downloading files.	
6. Stronger Passwords	15 min	Teacher explains the importance of using strong passwords and the steps to create a strong password.	Students understand the importance of using strong passwords and the steps to create a strong password.	
7. Understanding Abusive Content	15 min	Teacher discusses the risks of abusive content and the importance of reporting it.	Students understand the risks of abusive content and the importance of reporting it.	
8. Cyber Bullying	15 min	Teacher discusses the risks of cyberbullying and the importance of reporting it.	Students understand the risks of cyberbullying and the importance of reporting it.	
9. Summary and Reflection	10 min	Teacher summarizes the module and encourages students to reflect on what they have learned.	Students reflect on what they have learned and share their thoughts.	

Lesson Plan 2 - Game Based Learning				
Activity	Time	Details	Learning Goal	Notes
1. Introduction to the Game	10 min	Teacher introduces the game and its objectives. Students share their expectations for the game.	Students understand the game's goals and objectives.	
2. Game Play	30 min	Students play the game, which focuses on identifying and reporting cyber incidents.	Students apply their knowledge of cyber security concepts in a game-based learning environment.	
3. Reflection and Discussion	15 min	Teacher facilitates a discussion about the game, asking students to share their experiences and what they learned.	Students reflect on their game experience and share their learning.	
4. Summary and Reflection	10 min	Teacher summarizes the game and encourages students to reflect on what they have learned.	Students reflect on what they have learned and share their thoughts.	

Lesson Plan 3 - Consolidation				
Activity	Time	Details	Learning Goal	Notes
1. Review of Key Concepts	10 min	Teacher reviews the key concepts covered in the module, including the basics of cyber security, online behavior, reporting and recovery, when the internet lies, stronger passwords, understanding abusive content, and cyberbullying.	Students review and reinforce their understanding of the key concepts.	
2. Consolidation Activity	20 min	Students complete a consolidation activity, which involves applying their knowledge of cyber security concepts to a real-world scenario.	Students apply their knowledge of cyber security concepts to a real-world scenario.	
3. Reflection and Discussion	15 min	Teacher facilitates a discussion about the consolidation activity, asking students to share their experiences and what they learned.	Students reflect on their consolidation activity and share their learning.	
4. Summary and Reflection	10 min	Teacher summarizes the consolidation activity and encourages students to reflect on what they have learned.	Students reflect on what they have learned and share their thoughts.	

Lesson Plan 4 - Assessment				
Activity	Time	Details	Learning Goal	Notes
1. Introduction to the Assessment	10 min	Teacher introduces the assessment and its objectives. Students share their expectations for the assessment.	Students understand the assessment's goals and objectives.	
2. Assessment Activity	30 min	Students complete the assessment, which consists of a series of questions designed to test their understanding of the module's content.	Students demonstrate their understanding of the module's content through the assessment.	
3. Reflection and Discussion	15 min	Teacher facilitates a discussion about the assessment, asking students to share their experiences and what they learned.	Students reflect on their assessment experience and share their learning.	
4. Summary and Reflection	10 min	Teacher summarizes the assessment and encourages students to reflect on what they have learned.	Students reflect on what they have learned and share their thoughts.	

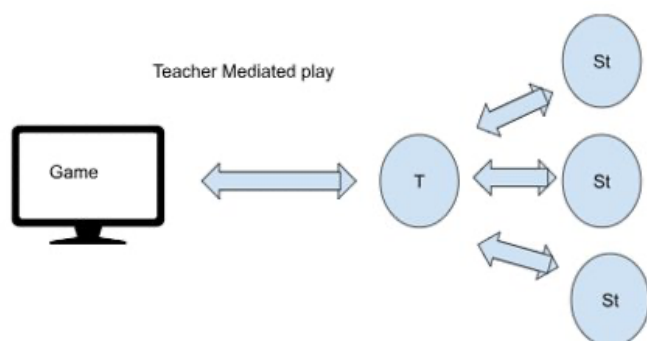
### 3.5.2 Details about the 7 modules that contain a lesson plan

- Module 1: Basics of Cyber Security
  - Goals:
    - The topic of cyber security
    - Discussing some of the basic activities people can do to make themselves safer
  - Topics:
    - Taking care of devices
    - Understanding and creating effective passwords
- Module 2: Online Behaviour
  - Goals:
    - The topic of online behaviour
    - Discussing how behaviour online should not differ from everyday life, how everyone should be polite
    - Introducing the topic of online bullying
  - Topics
    - The concept of netiquette
    - Appropriate online behaviour
    - Online bullying and responding to that behaviour
- Module 3: Reporting and Recovery
  - Goals:
    - The topic of reporting and recovery - what to do when something happens?
    - Discussing different reporting possibilities
  - Topics:
    - Lost device prevention and reporting
    - Lost money prevention and reporting
    - Basic hacking prevention and recovery
- Module 4: When the Internet Lies
  - Goals:
    - Discussing the basics of online fake information
    - Introducing different forms fake information can take
  - Topics:
    - Online purchases and wrong information
    - Fake people and profiles online
    - AI generated false information
- Module 5: Stronger Password
  - Goals:
    - strategies for protecting against cyber attackers
    - detecting and implementing actions against basic cyber-attacks
    - understanding basic cyber threats
    - basic prevention technologies
    - using software tools to protect digital devices
    - strategies to protect their personal information while surfing the web
  - Topics:
    - basics of cryptography
    - definition of password
    - how to create a good password
- Module 6: Understanding Abusive Content

- Goals:
  - detecting and acting against suspicious emails
  - what personal data is
  - phishing attacks
  - classifying abusive content
  - threats associated with personal data
  - identifying and protecting against untrue or untrustworthy information sources found online
  - online etiquette and behavior
  - classifying abusive content.
- Topics:
  - Definition of «hater» and «troll»
  - Differences between a real and fake profile
  - Good practices for sharing data online
- Module 7: Cyber Bullying
  - Goals:
    - understanding basic cyber threats
    - responding to inappropriate content by taking the correct actions
    - using strategies to protect against and prevent cyberbullying
    - utilizing strategies to stay safe in online social contexts
    - strategies to identify online frauds
    - classifying abusive content.
  - Topics
    - Definition of «hater» and «troll»
    - Definition of Malware
    - Introduction to risks of online gambling and game addiction

### 3.5.3 Game Based Approach

The program uses a game-based approach, where the game is played collaboratively with the teacher guiding the session. This format is ideal for large classrooms and is especially suitable for environments with limited access to technology.



## 3.6 The Platform

### 3.6.1 Platform Landing Page

- Go to: <https://platform.supercyberkids.eu/>

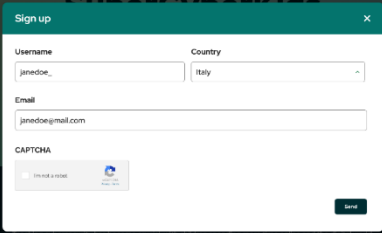
Click here to login if you are already registered

Click here to register on the platform



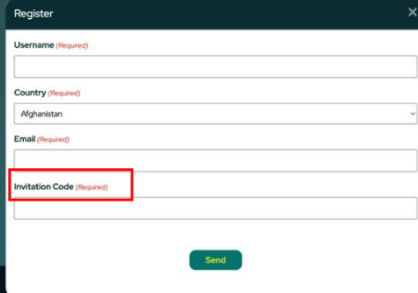
### 3.6.2 How to register (standard use)

- Enter your username, country and email.
- You will receive an email message with your TEMPORARY password.
- Once you log in to the platform, you will be asked to change the password to one of your choice.



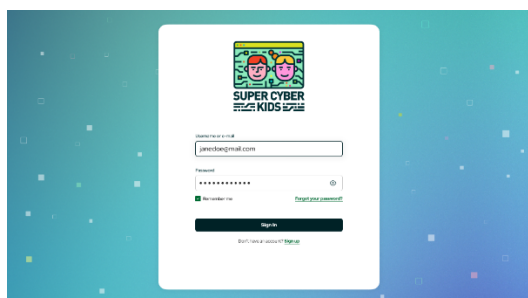
### 3.6.3 How to register for the SuperCyberKids Pilot testing (invitation only)

- You will need an INVITATION CODE to register on the platform.
- Your Country reference SuperCyberKids Manager will provide you with this code.
- You will receive an email message with your TEMPORARY password.
- Once you log in to the platform, you will be asked to change the password to one of your choice.



### 3.6.4 Log in to the platform

- If you have already registered on the platform, enter your username and your password.





### 3.6.5 The Platform's Home Page

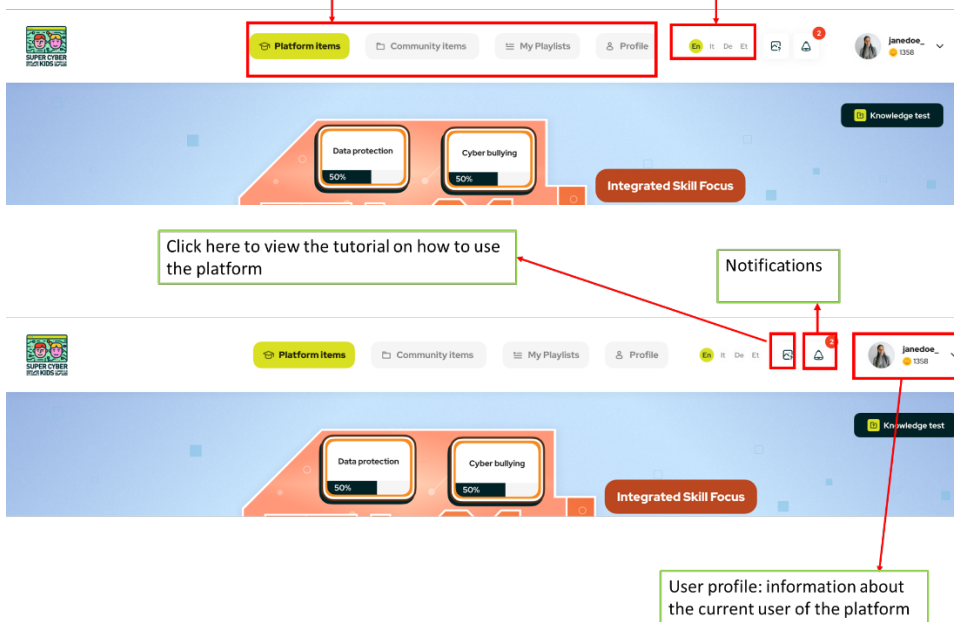
- This is the platform home page.
- It shows a visual map of the PLATFORM ITEMS: the 18 modules that make up the learning resources on cybersecurity developed or approved by SuperCyberKids.
- It is divided into three focus areas, distinguished by colour:
  - Technical Skills (green)
  - Social Skills (blue)
  - Integrated Skills (orange)



### 3.6.6 The Navigation Menu

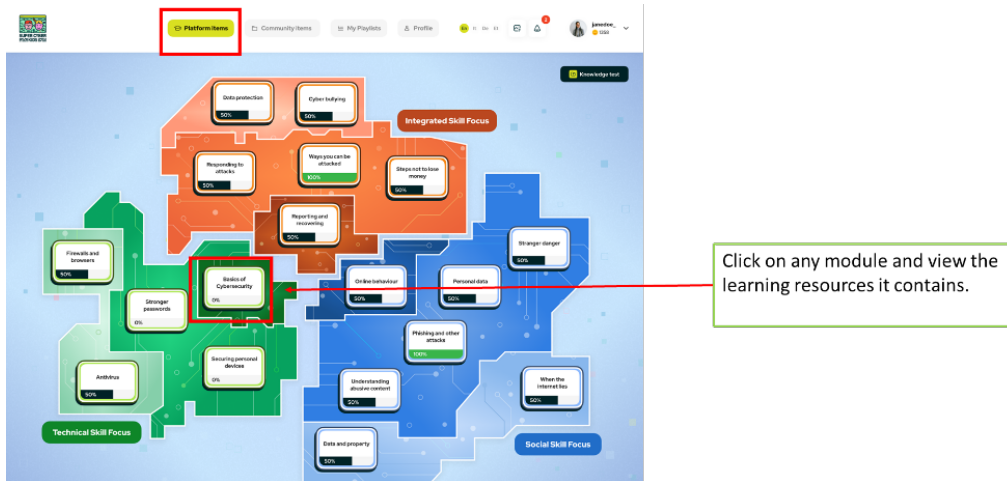
In the top navigation bar you will find the platform's main menu. Click on the items in the menu to navigate the platform.

Language selection



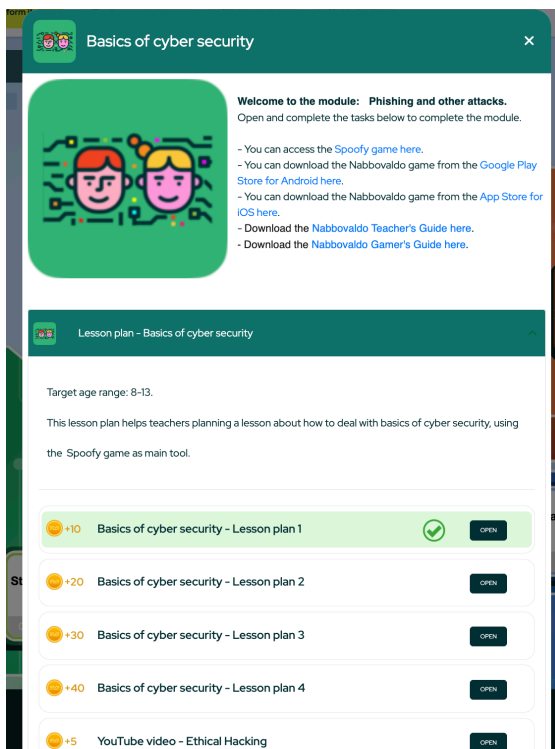
### 3.6.7 Platform Items

- The 18 modules are arranged by focus but also by level.
- The darker background in the centre denotes basic level, while lighter backgrounds towards the outside denote more advanced levels.



### 3.6.8 A SuperCyberKids Module

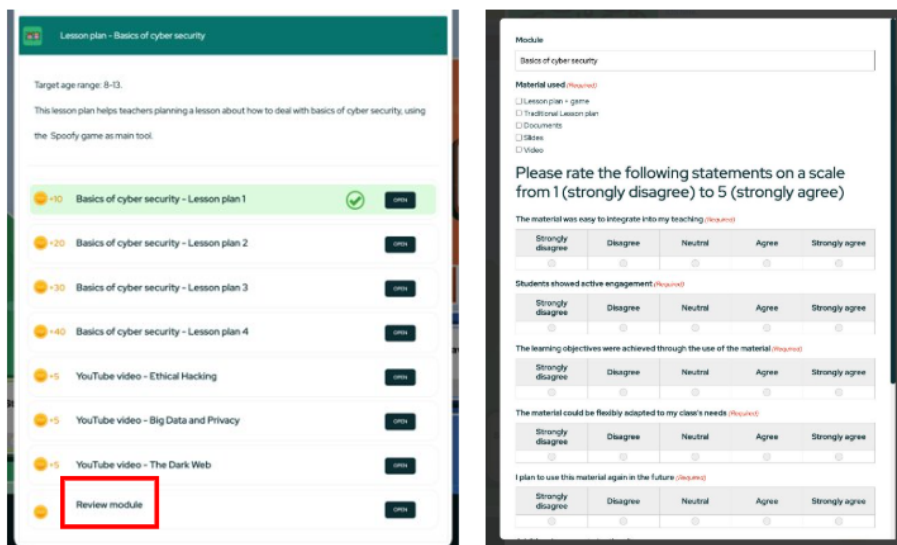
- Each module contains four Lesson Plans dedicated to that topic:
  - Introduction
  - Game Based Learning
  - Consolidation
  - Assessment
- You can open or print the Lesson Plan.
- Modules can also include links to games, video tutorials and other resources.
- Important: we are using 2 games currently with the lessons plan: Spoofy Game and Nabbovaldo Game.





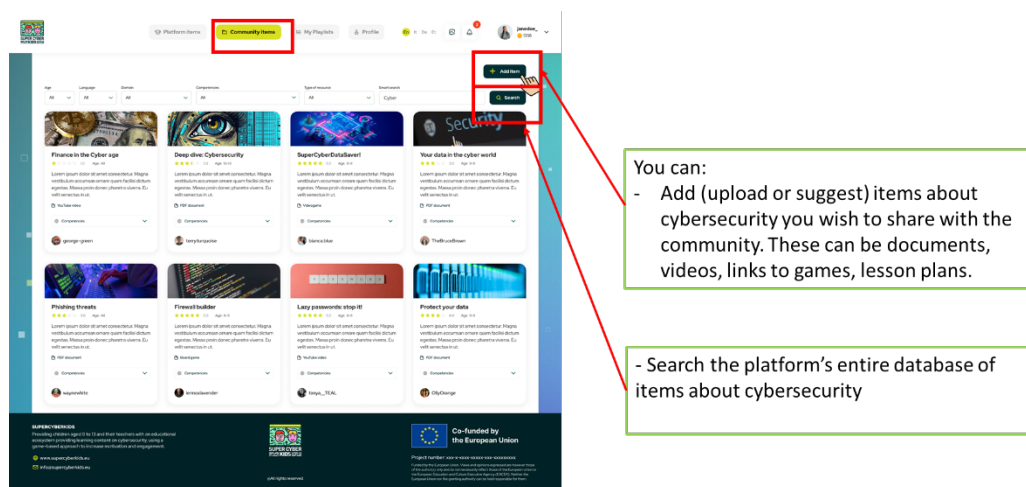
### 3.6.9 Feedback form

At the end of each module there is a link to the Feedback form. Here teachers can rate the material they have used and provide comments.



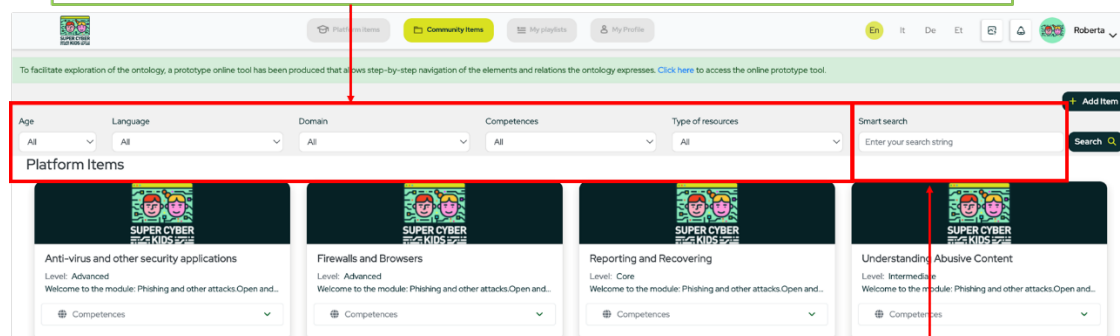
### 3.6.10 Community Items

This page contains the items suggested or uploaded by members of the SuperCyberKids user community.

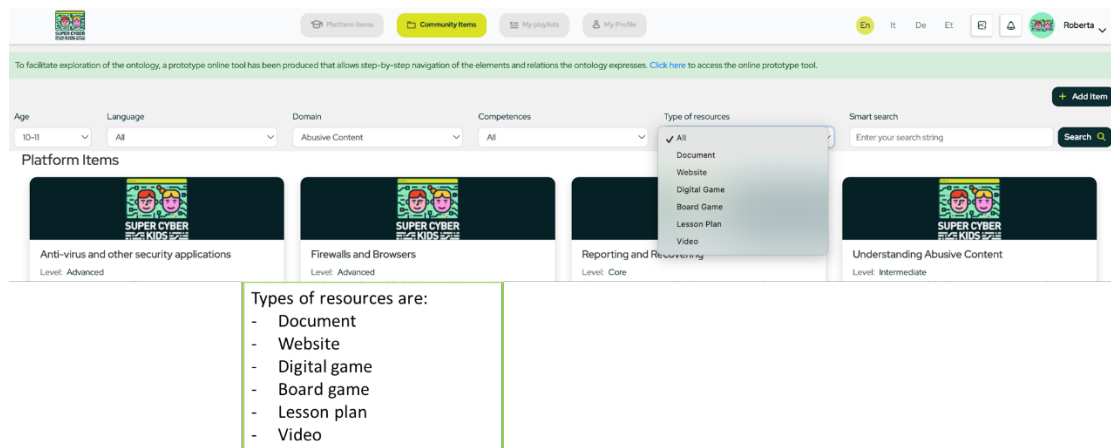


### 3.6.11 Search Function

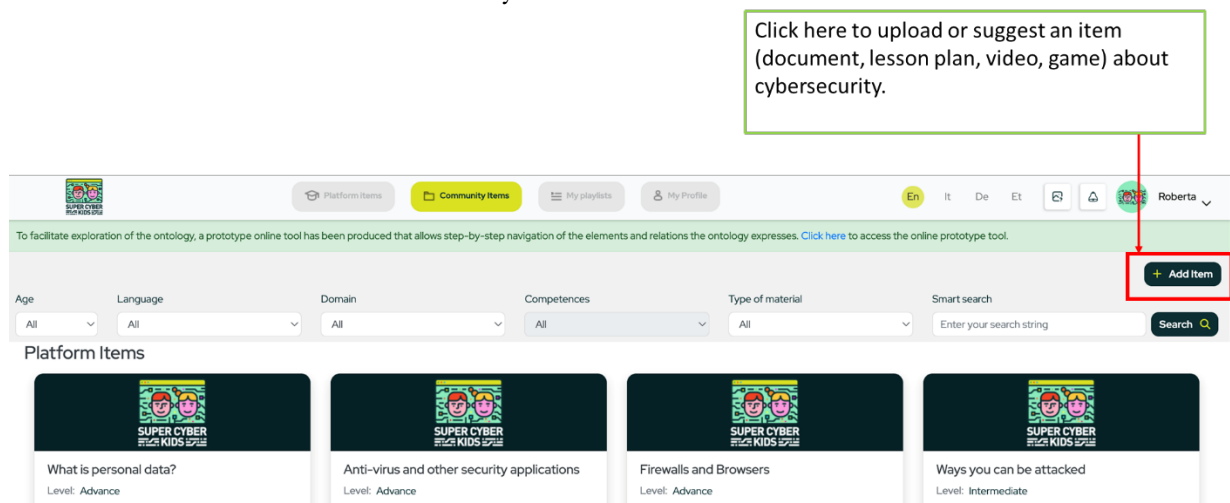
You can filter your search using these search criteria: age, language, competence domain and related competencies, type of resources



Here you can type keywords for your search. The platform has AI-enhanced features that will optimise the list of results you get from your search .



### 3.6.12 Add item to the Community



### 3.6.13 Add item to share it with the Community

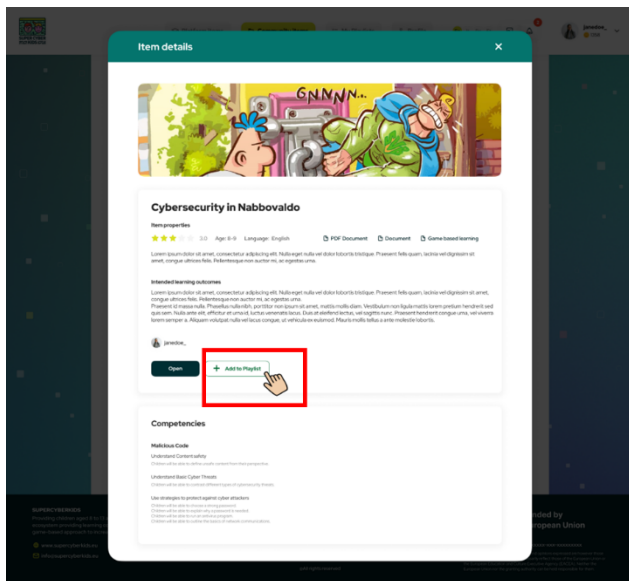
As well as providing a name and short description, it's helpful to add as many tags as possible to the item you're suggesting or uploading.

- item type (either a file or a link to an external resource)
- type of resource (lesson plan, document, video, game)
- style of lesson (game-based learning, traditional classroom, other)
- age
- language
- related cybersecurity competencies

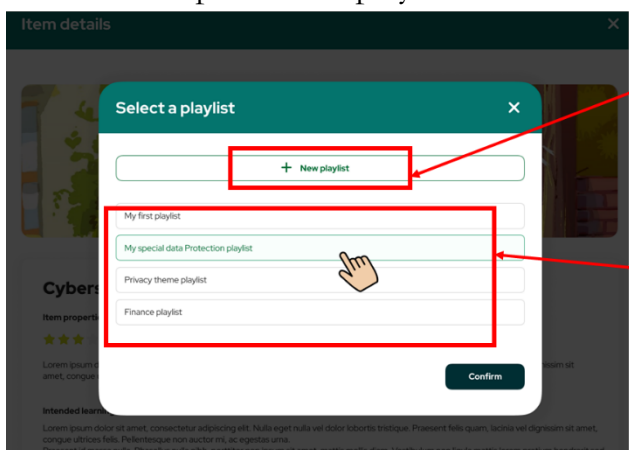
The screenshot shows the 'Add an Item' form. It has a green header with the title 'Add an Item' and a close button. The form contains several fields: 'Item Name', 'Item Description', 'Item Type' (External Link), 'Type of resources' (Digital Game), 'Style Of Lesson' (Game-based learn), 'Age' (10-11), 'Lang' (English), 'Item Uri', and 'Repository Item Image' (with a 'Select Image' button). Below these fields is a section for 'Item Intended Learning Outcomes'. At the bottom, there are two sections: 'Malicious code' and 'Safety', each with a list of checkboxes for specific competencies.

### 3.6.14 Add item to playlist

- In the «card» showing the details of the item added to the platform, you can select «Add to playlist» to add this particular item to a personal playlist of resources



### 3.6.15 Select or create a playlist

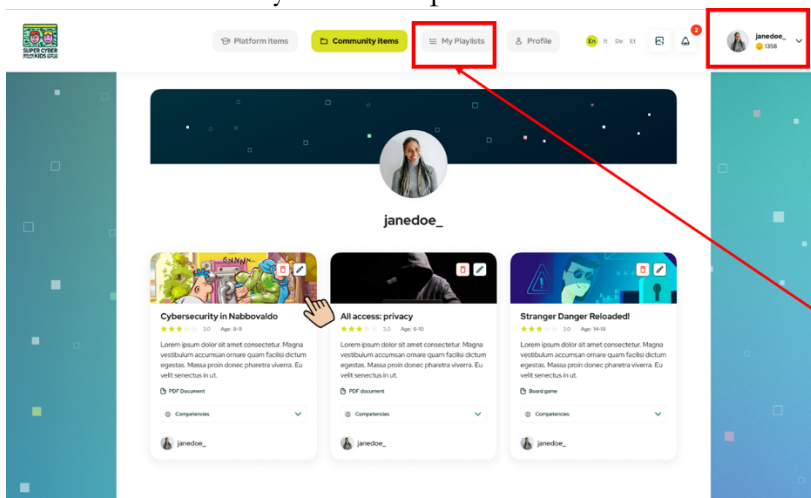


Click here to create a new playlist.

Here you can view all the playlists you have already created.

Select one of them and click on Confirm to add the new item to the selected playlist.

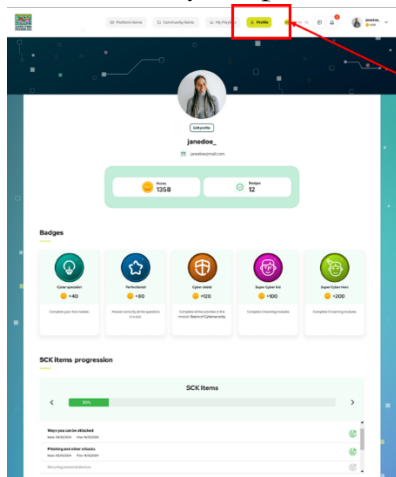
### 3.6.16 View items you have uploaded



Click here to view the items you have uploaded or suggested to the platform (My items).

Click here to view your playlists.

### 3.6.17 View your profile



Click here to view information related to your profile.

Here you can

- upload a profile photo
- view the badges you have achieved related to your progress in the platform
- view the Platform items you have browsed.

## 3.7 Assessment of Student Achievement

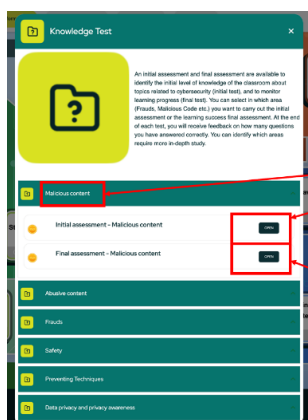
### 3.7.1 Knowledge test about Cybersecurity

- Use the test to identify the initial level of knowledge of the whole class about topics related to cybersecurity (initial test), and to monitor learning progress (final test).



Click here to open the Knowledge Test about Cybersecurity

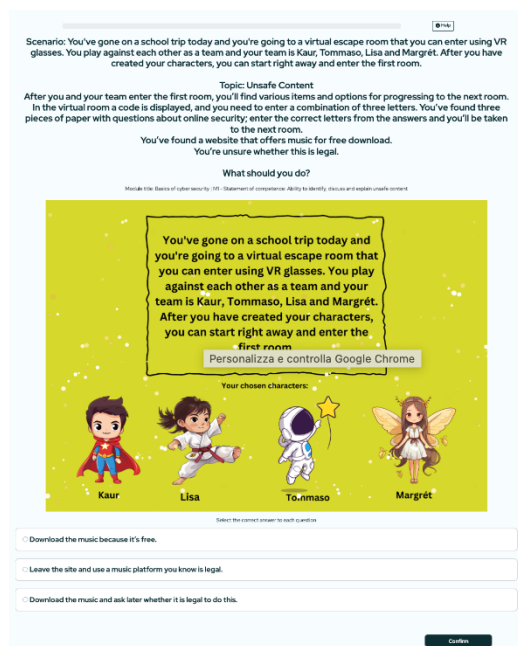
- The Knowledge test is divided into 6 parts, one for each domain of competencies on cybersecurity identified by SuperCyberKids.



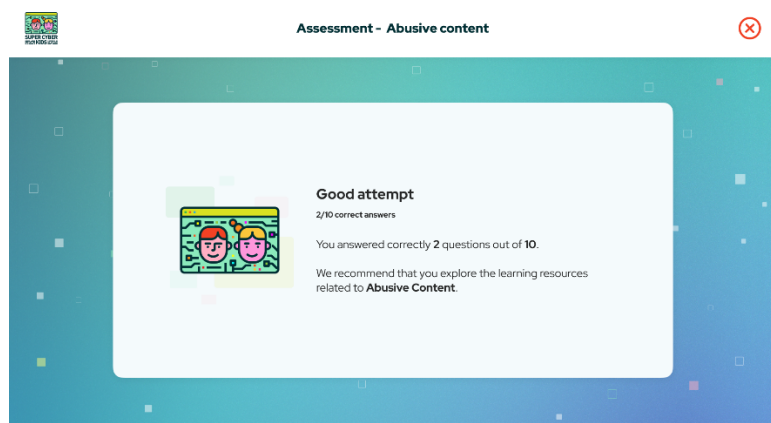
Select the domain in which you want to test the class's knowledge and then launch the test.

Click here to open the Final Assessment: you can run this test at the end of classroom activities to check students' learning progress.

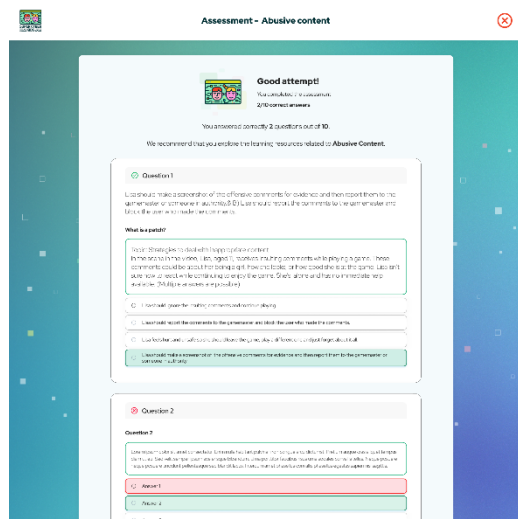
- Example of question and answers in the test about Malicious Content.
  - Questions embedded in scenarios
  - Multiple choice answers



- At the end of the initial test, the results panel shows the number of correct answers the class has given, and (when appropriate) a recommendation to view the related learning module.



- At the end of the Final test you will see all the correct answers to the questions in the test (in green) compared to the wrong answers (in red).



## 3.8 Modules

The presentations also include a short introduction to all 7 modules (see mentioned in 2.5.2).






This can be found in the presentation links in the Annex, called '07\_TT Intro Modules\_1\_2\_3\_4\_v1' & '08\_TT Intro Modules\_5\_6\_7\_v1'.




## 3.9 Next Steps for participating in the Pilot Phase

- To participate in the pilot phase, please inform us via email with the module you plan to teach.
- After we receive your selection, we will send you a login code to access the platform (Landing Page – Super Cyber Kids).
- A questionnaire will be provided after the pilot phase to help evaluate its value (probably again via LimeSurvey)



## 4 Appendix

### 4.1 General Powerpoints

	Powerpoint
01_General introduction to CyberSecurityEducation	 01_General%20intro duction%20to%20Cyt
02_The SuperCyber Kids Learning Framework_	 02_The%20SuperCyb er%20Kids%20Learnii
03_The SCKLF Competencies Explorer	 03_The%20SCKLF%2 0Competencies%20Ex
04_SuperCyberKids pilot ppt draft_split	 04_SuperCyberKids% 20pilot%20ppt%20dr
05_The Assessment of the Student's Achievements (1)	 05_The%20Assessme nt%20of%20the%20S

<b>06_SuperCyberKids platform training_v1</b>	 06_SuperCyberKids% 20platform%20trainir
<b>07_TT Intro Modules_1_2_3_4_v1</b>	 07_TT%20Intro%20M odules_1_2_3_4_v1.pptx
<b>08_TT Intro Modules_5_6_7_v1</b>	 08_TT%20Intro%20M odules_5_6_7_v1.pptx

## 4.2 Powerpoints of each pilot

	<b>Powerpoint</b>
<b>Italian Pilot</b>	CNR-ITD\SuperCyberKids - WP6 - Implementation of pilot use cases in schools\PPTs for teacher training\[ITA] Translation
<b>Estonian Pilot</b>	 Supercyberkids%20sl ides%20EST.pptx
<b>German Pilot</b>	CNR-ITD\SuperCyberKids - WP6 - Implementation of pilot use cases in schools\PPTs for teacher training\[GER] Translation
<b>EU-based Pilot</b>	 SCK_Teacher%20Trai ning.pptx



### 4.3 Lessonplans of each module

	Lessons Plan 1 (Introduction)	Lessons Plan 2	Lessons Plan 3	Lessons Plan 4
<b>Abusive Content</b>	 SCK-lesson_plan_Abusive%20Content_lesson1.docx	 SCK-lesson_plan_Abusive%20Content_lesson2.docx	 SCK-lesson_plan_Abusive%20Content_lesson3.docx	 SCK-lesson_plan_Abusive%20Content_lesson4.docx
<b>Basics of Cybersecurity</b>	 SCK-lesson_plan_BasicsCybersecurity_lesson1.docx	 SCK-lesson_plan_BasicsCybersecurity_lesson2.docx	 SCK-lesson_plan_BasicsCybersecurity_lesson3.docx	 SCK-lesson_plan_BasicsCybersecurity_lesson4.docx
<b>Cyberbullying</b>	 SCK-lesson_plan_CyberBullying_lesson1.docx	 SCK-lesson_plan_CyberBullying_lesson2.docx	 SCK-lesson_plan_CyberBullying_lesson3.docx	 SCK-lesson_plan_CyberBullying_lesson4.docx
<b>Online Behaviour</b>	 SCK-lesson_plan_OnlineBehaviour_lesson1.docx	 SCK-lesson_plan_OnlineBehaviour_lesson2.docx	 SCK-lesson_plan_OnlineBehaviour_lesson3.docx	 SCK-lesson_plan_OnlineBehaviour_lesson4.docx
<b>Reporting and recovering</b>	 SCK-lesson_plan_Reporting%20Recovering_lesson1.docx	 SCK-lesson_plan_Reporting%20Recovering_lesson2.docx	 SCK-lesson_plan_Reporting%20Recovering_lesson3.docx	 SCK-lesson_plan_Reporting%20Recovering_lesson4.docx
<b>Stronger Passwords</b>	 SCK-lesson_plan_StrongerPasswords_lesson1.docx	 SCK-lesson_plan_StrongerPasswords_lesson2.docx	 SCK-lesson_plan_StrongerPasswords_lesson3.docx	 SCK-lesson_plan_StrongerPasswords_lesson4.docx
<b>When the Internet lies</b>	 SCK-lesson_plan_InternetLies_lesson1.docx	 SCK-lesson_plan_InternetLies_lesson2.docx	 SCK-lesson_plan_InternetLies_lesson3.docx	 SCK-lesson_plan_InternetLies_lesson4.docx