Handbook of good practices on cybersecurity education in schools for children aged 8-13

SuperCyberKids
D7.1

Call: ERASMUS-EDU-2022-PI-FORWARD
Type of Action: ERASMUS-LS
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.

Project ref. number	101087250
Project title	**SCK - SuperCyberKids**
Document title	Handbook of good practices on cybersecurity education in schools for children aged 8-13
Document Type	Deliverable
Document version	2, 30.1.2026
Previous version(s)	1,22.12.2025
Planned date of delivery	31.12.2025
Language	English
Dissemination level	Public
Number of pages	48
Partner responsible	CNR
Author(s)	Manuel Gentile, CNR;
With contributions by:	Dirk Ifenthaler, UMA; Erica Melloni, AVANZI
Revised by:	Jeffrey Earp, CNR; Dirk Ifenthaler, UMA. Roberta Memeo, GRIFO, Ilaria Matteucci, CNR; Giuseppe Città, CNR
Abstract	This deliverable presents the SuperCyberKids Handbook of good practices for cybersecurity education in schools, aimed at children aged 8–13, and includes operational recommendations for researchers, teachers, parents, designers/developers and policy makers. The document integrates and updates the guidelines previously defined in the project (skills framework, curriculum map and design guidelines), relating them to the evidence gathered during teacher training activities and classroom testing of games, platforms and lesson plans. Through a synthesis process combining documentary analysis and qualitative analysis of teacher feedback, effective practices are identified for designing age-appropriate teaching resources, orchestrating classroom activities with sustainable timings, promoting continuity between school and home, and supporting adoption through support materials and monitoring tools. Recommendations for teachers, parents and designers aim to support co-design processes centred on pupils' needs; those for policy makers provide guidance on how to integrate the framework into the formal curriculum in a more informed way, with a focus on training, implementation and scalability of the SuperCyberKids ecosystem.
Keywords	SuperCyberKids; Cybersecurity education; good practices
DOI	https://doi.org/10.17471/54037
How to cite	Gentile, M. (2025). Handbook of good practices on cybersecurity education in schools for children aged 8-13. Deliverable 7.1 - SuperCyberKids project (ERASMUS-EDU-2022-PIFORWARD - ERASMUSLS - Project No. 101087250). DOI: https://doi.org/10.17471/54037

Internal project peer review process

Approved by		
Manuel Gentile	Project Coordinator (CNR-ITD)	22/12/2025
Jeffrey Earp	CNR-ITD	16/01/2026

Table of Contents

Index of tables 6
1 Introduction 7
1.1 The SuperCyberKids Project Context 7
1.2 Purpose and Scope of the Handbook 7
1.3 Structure of the Handbook 8
2 Methodology 8
3 From Framework to Practice: Building on Previous Work 10
3.1 The SuperCyberKids Learning Framework (D2.1): conceptual foundations, skills, and ontology 10
3.1.1 Methodological approach to framework construction 11
3.1.2 The SCKLF ontology: structure, function, and added value 12
3.2 Principles and structure of the cybersecurity education curriculum (D3.1) 12
3.3 Guidelines for the design and adaptation of educational cybersecurity games (D4.3) 13
4 What works in practice: evidence from the field 14
4.1 Structure and objectives of the pilot phase 15
4.2 Implementation and adaptation models in the various pilot projects 15
4.3 Participation scale and ecological validity 16
4.4 Results from teachers' pre-training survey 17
4.5 Results from teachers' post-training survey 22
4.6 Results from teachers' post pilot survey 25
4.7 Challenges and recommendations expressed by teachers 27
5 Evidence-based good practices 28
5.1 Good Teaching Practices 28
5.2 Good Educational Design Practices 30
5.3 Good Organizational Practices 31
5.4 Summary 31
6 Recommendations for key stakeholders 32
6.1 Recommendations for teachers and schools 32
6.2 Recommendations for parents and families 34
6.3 Recommendations for educational game designers and developers 35
6.4 Recommendations for researchers 38
6.5 Recommendations for policymakers and education authorities 40
7 Pathways to implementation 41

7.1 An implementation roadmap: from the "minimum sustainable" to scaling 42
7.1.1 Phase 1 – Start-up 42
7.1.2 Phase 2 – Consolidation 42
7.1.3 Phase 3 – Extension and scaling 43
7.2 Roles and responsibilities 43
7.3 SuperCyberKids Enactment Tool revised 44
7.4 Minimum adoption and quality indicators 45
7.5 Curriculum and framework alignment: how to make it explicit 45
7.6 Operational recommendations for policy and governance (implementation summary) 47
8 Conclusions 47

Index of tables

Table 1: Responses by country of origin 17
Table 2: Which subject do you teach? 17
Table 3: Which subject do you teach (by country)? 18
Table 4: Age range of students taught 18
Table 5: Integration of cybersecurity education – by country 18
Table 6: Familiarity with cybersecurity concepts and perceived urgency of cybersecurity education (% of total respondents, unified scale) 19
Table 7: Perceived urgency of cybersecurity education – by country 19
Table 8: Importance of teaching cybersecurity vs. confidence in teaching it 19
Table 9: Confidence in teaching cybersecurity (Not at all + Slightly) 20
Table 10: Inclusion of cybersecurity topics in lessons – by country (% within each country) 20
Table 11: How familiar are you with the concepts of gamification and using games in education? 20
Table 12: Do you use gamification and games in your teaching practices? 20
Table 13: post-training survey response rates by country 22
Table 14: Timing of participation in the training activities 22
Table 15: Age range of students taught 23
Table 16: Subjects taught 23
Table 17: overall rating of SuperCyberKids training and preparedness to use SuperCyberKids resources after training 23
Table 18: training programme satisfaction by country 24
Table 19: teachers' post pilot survey response rates 25
Table 20: Teacher-reported student response to the SuperCyberKids experience 25
Table 21: resource types considered most useful in the SuperCyberKids experience 26
Table 22: Type of SuperCyberKids learning resource rated by engagement 27
Table 23: Recommendations for teachers and schools 33
Table 24: Quick checklist for teachers and schools 34
Table 25: Recommendations for parents and families 35
Table 26: Quick checklist for parents and families 35
Table 27: Recommendations for designers and developers 37
Table 28: Quick checklist for designers and developers 38
Table 29: Recommendations for researchers 39
Table 30: Quick checklist for researchers 39
Table 31: Recommendations for policymakers and education authorities 40
Table 32: Quick checklist for policymakers and education authorities 41
Table 33: SuperCyberKids implementation roadmap 42
Table 34: Roles and responsabilities matrix 44

1 Introduction

1.1 The SuperCyberKids Project Context

The SuperCyberKids (SCK) project responds to the growing need to support cybersecurity education for children aged 8–13 by creating, testing and evaluating a game-based learning ecosystem. As children's engagement with digital technologies becomes increasingly early, frequent and autonomous, cybersecurity education can no longer be postponed to later stages of school or reduced to technical notions or isolated awareness campaigns. Instead, it must be integrated with pedagogically valid, developmentally appropriate and ethically responsible learning experiences.

The project has progressively generated a series of results providing the conceptual and operational basis for the development and piloting of the SuperCyberKids ecosystem. This process began with the SuperCyberKids Learning Framework (SCKLF) (Deliverable D2.1). This defines a competency-based cybersecurity education model grounded in an ontological approach, identifying domains, competencies, and skills relevant to the 8–13 age group. Building on this framework, an EU reference framework (Deliverable D3.1) was proposed to integrate game-based cybersecurity education into formal school curricula. It encompasses institutional, pedagogical and assessment dimensions from the perspective of schools and education authorities. Additionally, methodological guidelines for game designers were laid out (Deliverable D4.3), supporting competence-oriented design and adaptation of serious games and learning activities in line with the SCKLF.

All these results establish the theoretical, regulatory and design-oriented pillars of the SuperCyberKids approach. This handbook addresses a complementary but essential dimension: the systematic consolidation of empirical evidence from classroom testing of the SuperCyberKids platform and content, associated support materials, and the SuperCyberKids ecosystem feasibility for adoption in schools. It summarises and analyses the findings from teacher training activities, pilot implementations, and in-depth interviews with teachers who have implemented SuperCyberKids tools and resources in real school settings.

1.2 Purpose and Scope of the Handbook

The main objective of this handbook is therefore twofold. First, it identifies and articulates evidence-based good practices for cybersecurity education with children aged 8 to 13. This entails focusing on pedagogical strategies, orchestration models, activity design, assessment approaches, and contextual constraints encountered in everyday school practice. Secondly, these practices are fashioned into practical suggestions for various stakeholder groups, including teachers, parents, game designers, researchers, and policymakers.

Regarding teachers, parents, and designers, the handbook aims to support the adoption and implementation of the overall SuperCyberKids ecosystem as a whole. This regards co-design of high-quality teaching resources, with the spotlight on conditions that improve teaching effectiveness, such as guided reflection, age differentiation, modular lesson structures, and the pedagogical mediation of game-based activities. Rather than promoting games as stand-alone solutions, the handbook emphasises the importance of integrating game-based tools into structured learning pathways, supported by explicit teaching guidance and reflective discussion. For policymakers and educational authorities, the handbook provides empirically based guidance for the formal integration of cybersecurity education into school curricula.

The recommendations presented in this document complement and substantiate the policy guidelines provided in Deliverable D3.1 by basing curriculum integration strategies on enacted classroom practices, teacher feedback, and institutional concerns and constraints. This evidence-based perspective supports more informed decision-making regarding scalability, sustainability, and alignment with existing curriculum frameworks.

It is important to emphasise that this handbook does not introduce a new theoretical framework within SuperCyberKids. It rather serves as a bridge between the foundational theoretical framework and classroom reality, validating, refining, and contextualising the principles previously defined in the project. By systematically incorporating practitioners' perspectives, the handbook helps bridge the gap between intended educational design (informed by extensive investigation and analysis of the scientific literature) and implemented educational practice.

1.3 Structure of the Handbook

The handbook's structure reflects this purpose. Following an overview of the methodological background of the SuperCyberKids initiative, the handbook presents a summary of the key findings that emerged from pilot experiences and teacher interviews. To enhance applicability, these findings are organised around recurring pedagogical themes and challenges. They are then translated into a series of good practices and recommendations, which are expressed both in concise, operational form and as narratives. This two-fold description is intended to facilitate interpretation and foster transfer between different contexts. The concluding sections clearly set out the implications for different stakeholder groups, reinforcing the collaborative, ecosystem-oriented vision that underpins the SuperCyberKids project.

In summary, this handbook gives a theoretical and practical overview of the exploration, educational design, and experimentation work carried out in the SuperCyberKids project. It is an evidence-based guide that consolidates research, design and practice and supports the sustainable adoption of cybersecurity education for children aged 8–13 in different educational contexts.

2 Methodology

The methodology for producing this handbook was designed to ensure that the good practices and recommendations presented in this document are empirically grounded, contextualised and relevant to the various stakeholders potentially involved in the SuperCyberKids ecosystem.

In line with the handbook's objectives, the methodological approach organises and critically interprets the data collected during the training, testing, and evaluation activities carried out in the project, relating these to the theoretical and design frameworks defined in the early stages of the project and reported in previous deliverables.

Evidence was gathered through situated implementations integrated into ordinary school practice to observe feasibility, adoption conditions, and instructional dynamics under real constraints (time, infrastructure, curricular variability, and heterogeneous teacher competences). The pilot phase (WP6) ran between January and November 2025 and was organised as four localised case studies:

- Italy
- Estonia
- Germany
- EU-wide pilot conducted in English

Across contexts, pilots followed a shared structure combining standardisation and local adaptation to test ecosystem robustness and scalability:

- Teacher training (online or hybrid), focused on the SuperCyberKids Learning Framework (SCKLF), lesson plans, platform use, and curricular integration strategies.
- Classroom testing of selected ecosystem modules, chosen voluntarily by teachers and adapted to local organisational and pedagogical needs.
- Systematic feedback collection through pre-training, post-training and post-pilot questionnaires, complemented by post-pilot teacher interviews.

Pilot actions also involved school leaders, recognising their strategic role in adoption, organisational enablement, and longer-term curricular consolidation of cybersecurity education.

The handbook is based on complementary evidence streams that enable triangulation between design intentions, user experience, and situated classroom practice:

- Training feedback (including structured questionnaires administered before and after training activities);
- Post-pilot teacher questionnaires capturing perceived effectiveness, usability and implementation constraints;
- Semi-structured post-pilot teacher interviews eliciting in-depth reflections on classroom orchestration, student engagement, challenges, and enabling conditions.

Teacher training was a crucial phase in the methodological process. It was not conceived as a simple transfer of content but as a moment of pedagogical mediation between the project's theoretical framework and teaching practice. During the training, teachers were introduced to the principles of the SuperCyberKids Learning Framework (SCKLF) and the pedagogical logic underlying the tools and games initially integrated into the ecosystem. Attention was paid to how to integrate learning resources into curricular activities.

Following the training phase, teachers were invited and supported to experiment with SuperCyberKids tools in their classrooms, adapting them to organisational drivers and constraints, student characteristics, and established teaching practices. This phase allowed us to observe how the design of the tools and accompanying resources can impact situated educational practices, often through a natural phase of adaptation, simplification and/or possible reorganisation.

Before and after the participant training phase, structured data was collected through questionnaires. Questionnaires were also distributed to gather teachers' impressions of classroom experimentation.

Furthermore, at the end of the experimentation activities, semi-structured interviews were conducted with small teacher samples. The interviews were designed to encourage critical reflection on classroom experience, going beyond purely positive or negative evaluations of the tools and highlighting the conditions that affect the effectiveness of the practices adopted. Specifically, the interviews addressed the following topics in detail:

- how tools and resources were used in the classroom and combined with lesson plan activities;
- the teacher's role in mediating gameplay, guiding reflection and managing classroom dynamics;
- student reactions, engagement patterns and age-related differences;
- constraints encountered (technical, organisational, curricular) and strategies adopted to overcome them;
- perceived educational value and conditions for sustainable adoption.

These sources were synthesised in a complementary manner, enabling triangulation of evidence and the capture of both design aspects and the situational and contextual aspects of the educational experience.

Data were analysed through thematic analysis. Coding focused on recurring patterns across contexts (effective strategies, frictions, adaptation moves, and enabling conditions), with particular attention to teacher mediation, activity structuring over time, age-appropriateness, assessment and reflection practices, and contextual constraints. The analysis prioritised educational practices around the tools (how resources are orchestrated) rather than isolated tool features.

Transferable good practices and operational recommendations were derived through an explicit synthesis pipeline that links evidence to the handbook structure:

1. Pilot evidence is summarised and organised around recurring themes and challenges (Chapter 4);
2. Themes are consolidated into evidence-based good practices, expressed both narratively and in concise operational form (Chapter 5);
3. Good practices are re-articulated into stakeholder-specific recommendations (Chapter 6);
4. Recommendations are operationalised into implementation and scaling pathways (Chapter 7).

The evidence base is primarily qualitative and relies substantially on self-reported teacher data. The number and variety of contexts do not support statistical generalisation, and institutional and cultural specificities shape findings. Nevertheless, the situated nature of the pilots provides strong ecological validity and yields actionable guidance for transfer and scaling.

3 From Framework to Practice: Building on Previous Work

This chapter explains how the handbook (project Deliverable D7.1) builds on earlier SuperCyberKids results and clarifies the position of D7.1 in relation to deliverables D2.1, D3.1, and D4.3[1].

Specifically, the chapter explains how the coordinated application of the SuperCyberKids Learning Framework (SCKLF) with the principles of curricular integration and guidelines for educational design provides the intentional basis for the classroom experimentation practices. The chapter does not introduce new theoretical models. Still, it provides an integrated and practice-oriented reading of extant results, paving the way for analysis of the empirical evidence presented in the subsequent chapter.

3.1 The SuperCyberKids Learning Framework (D2.1): conceptual foundations, skills, and ontology

The SuperCyberKids Learning Framework (SCKLF), presented in Deliverable D2.1[2], is the main theoretical and conceptual reference point for the entire SuperCyberKids project. The framework has been developed to systematically define what it means to educate children aged 8 to 13 about cybersecurity, moving beyond fragmented, exclusively technical or single-tool-based approaches.

D2.1 provides a theoretical model that integrates a literature analysis, mapping of existing initiatives, references to European frameworks, and ontological modelling of competences.

In particular, the document aims to:

- identify the key domains of cybersecurity education relevant to the 8–13 age group;

[1] See https://www.supercyberkids.eu/deliverables/
[2] D2.1 – SuperCyberKids Learning Framework (SCKLF)

- define the competences and skills expected of children from a developmental rather than purely factual perspective;
- provide a solid conceptual basis for the design of games, educational activities and assessment tools;
- ensure alignment with European initiatives and frameworks on digital competences.

The framework provides a flexible reference structure that supports design, adaptation and integration in different educational contexts.

3.1.1 Methodological approach to framework construction

The construction of the SCKLF is based on a multi-pillar approach that combines:

- A systematic review of scientific literature, aimed at identifying cybersecurity skills relevant to children between 8 and 13.
- The analysis focuses on existing educational initiatives, both European and non-European, specifically examining their targets, areas of competence, and adopted educational methods.
- The comparative analysis of European frameworks for digital skills is conducted to ensure conceptual consistency and interoperability.

The results ere validated through a Delphi study involving experts in cybersecurity, education, and game-based learning.

This approach has enabled the development of an empirically grounded framework, avoiding both a purely theoretical drift and reliance on individual cases or tools.

One of the central contributions of D2.1 is the identification and structuring of the main domains of cybersecurity education for ages 8–13. The framework postulates that in general, but especially for this age group, cybersecurity cannot be reduced to technical skills but must include cognitive, social, and ethical aspects.

The main domains identified include:

- Data Privacy & Privacy Awareness
- Malicious Code & Cyber Attacks
- Fraud
- Preventing Technologies
- Abusive Content
- Safety

These domains cover both technical and social/behavioural risks, reflecting a broad view of cybersecurity as a digital citizenship skill.

Within the domains, the framework articulates a set of competences and skills, formulated in a consistent manner with a "can do" approach. The competencies do not simply describe what children should know but also what they should be able to do, understand, and recognise in concrete situations.

This approach:

- facilitates the design of educational activities and games;
- makes the link between learning and behaviour explicit;
- supports formative and reflective assessments.

However, translating these competences into effective teaching practices always requires strong educational mediation.

3.1.2 The SCKLF ontology: structure, function, and added value

A distinctive feature of Deliverable D2.1 is the development of a formal ontology for the SuperCyberKids Learning Framework. The ontology represents an explicit formalisation of the relationships between:

- cybersecurity domains
- competencies
- skills
- learning levels
- educational contexts.

From a conceptual perspective, the ontology makes the framework explicit, queryable and reusable, and supports the consistent design of educational content and games. Furthermore, it supports the design of educational technologies that ensure alignment between learning objectives, activities and assessments.

From an operational perspective, the ontology forms the basis for:

- the mapping of educational resources to skills;
- the internal consistency of the SuperCyberKids ecosystem;
- the scalability and future evolution of the framework.

It is important to note that the ontology is not intended to be used directly by teachers in the classroom but rather as a conceptual support infrastructure for designers, researchers, and developers.

3.2 Principles and structure of the cybersecurity education curriculum (D3.1)

Deliverable D3.1[3] translates the SuperCyberKids Learning Framework into a structured curriculum proposal designed to support the integration of cybersecurity education into formal school systems. Compared to D2.1, which defines domains, competencies and skills, D3.1 focuses explicitly on the curricular organisation of learning, addressing the question of how the acquisition of these competencies can be distributed over time, integrated into disciplines, and made sustainable at an institutional level.

The SuperCyberKids curriculum is conceived as a multi-level structure, operating on several complementary levels. At the first level, it is based on the SCKLF domains of competence, which serve as a stable conceptual reference. At the second level, these domains are translated into curriculum modules, which are understood as units of educational organisation that can be adapted, combined, and reused in different contexts. At the third level, the modules are translated into activities, resources and tools, including games and support materials.

A central aspect of D3.1 is the emphasis on curriculum modularity. The modules are not designed as rigid, linear sequences but as autonomous components that can be integrated at different points in the school curriculum. This allows schools to progressively implement the curriculum, overcoming the need for universal solutions that may prove challenging to align with the operational realities of classrooms. Modularity also responds to the need to adapt content and timing to different age groups and levels of maturity among students.

The curriculum progression proposed in D3.1 covers the entire age range of 8–13 years and is based on a principle of increasing cognitive complexity. In the early stages of the programme, the focus is primarily on identifying risky situations, gaining awareness, and learning basic rules. As students grow, the curriculum gradually introduces tasks that require interpreting situations, assessing consequences, and

[3] D3.1 – Reference framework for integration of the SCK game-based learning ecosystem on cybersecurity into school curricula – guidelines for schools

making responsible decisions. This progression provides a guide for designing programs that are consistent with students' development. Another important structural element of the SuperCyberKids curriculum concerns the cross-curricular dimension of disciplinary integration. D3.1 clarifies that cybersecurity skills do not necessarily have to be placed in a designated curricular space but can be developed within existing disciplines, particularly civic education, languages, social sciences, and technological areas. From this perspective, the curriculum acts as a glue, highlighting connections between cybersecurity learning objectives and subject objectives already present in national curricula. The topic of assessment is addressed in D3.1 as an integral part of the curriculum structure. In line with the SCKLF's competency-based approach, the curriculum favours formative and reflective assessment methods, focusing on observing behaviour, guiding discussions, and assessing students' ability to interpret and deal with realistic situations. Assessment is therefore not conceived as a separate event but as a component distributed throughout the curriculum. Finally, D3.1 clarifies the role of educational institutions and policymakers in making the curriculum effectively implementable.

The proposed structure assumes supportive conditions in terms of governance, teacher training, and alignment with educational policies, recognising that curriculum sustainability does not depend solely on the continuing availability of quality teaching materials.

3.3 Guidelines for the design and adaptation of educational cybersecurity games (D4.3)

Deliverable D4.3[4] completes the project's foundational pilars, being aimed specifically at game designers and developers, and designers of game-based learning activities. Remembering that the objective of SuperCyberKids is to create, test and evaluate a game-based learning ecosystem, the document addresses a central issue in the project: how to ensure that educational cybersecurity games are engaging, pedagogically sound, competence-oriented, and adaptable across different educational contexts.

D4.3 explicitly references the SuperCyberKids Learning Framework (D2.1) and extends its use beyond the definition of competences, proposing a systematic methodology to design, analyse, and adapt cybersecurity-themed educational games, both existing and newly developed, and their successful integration into the SuperCyberKids ecosystem.

The main contribution of D4.3 is the definition of a methodology that starts with games and leads to the design of contextualised learning activities in line with the principles of competence-based education. In this perspective, the game is not considered a self-sufficient object but an educational artefact to be integrated into a broader educational path.

The proposed methodology is divided into two main phases. The first phase focuses on mapping skills and consists of analysing the game content in relation to the skills and abilities defined in the SCKLF. This phase makes it possible to clarify the educational objectives supported by the game and to overcome the opacity that often characterises serious games from a pedagogical perspective. The second phase is dedicated to the design of educational activities, in which the game is placed within a teaching context, considering time, technological and institutional constraints.

A key element of D4.3 is the operational use of the SuperCyberKids Learning Framework ontology, already introduced in D2.1. This ontology is a tool for conceptual representation and a concrete support for game design and evaluation.

[4] D4.3 – Guidelines for game designers and developers: adaptation and localization of other applied games

Through the ontology, it is possible to explore domains, skills, abilities and relationships between concepts in a structured way. It facilitates the process of aligning game content with educational objectives. D4.3 explains how this approach allows designers to select specific competences, avoiding both overly broad coverage and random content focus. The ontology thus becomes a reference infrastructure that ensures consistency between frameworks, curricula and educational resources.

D4.3 devotes considerable space to the issue of evaluating game content, recognising that one of the main limitations of serious educational games is the lack of transparency regarding what they intend to teach. Starting with a scoping review of the literature, D4.3 proposes a multi-stage evaluation model that includes an initial phase to define objectives, a theoretical evaluation of the content, and practical validation through the end-user involvement. This approach allows verifying not only whether a game is potentially suitable for developing certain skills, but also whether those skills are exercised and consolidated during the gaming experience. Evaluation thus becomes an integral part of the design process, rather than an ancillary or post hoc activity.

Alongside analysis of existing games, D4.3 provides guidelines for the design of new educational games, based on the principles of competence-based education. The document emphasises the importance of making learning objectives explicit, designing game mechanics that allow students to demonstrate mastery of skills, and providing clear and meaningful feedback. Cross-cutting design aspects are also discussed, such as the type of learning supported by the game, genre and aesthetic choices, the appropriateness of content for the student age group, as well as legal and ethical constraints related to data collection and privacy protection. These elements reinforce the idea that designing educational games requires an integrated vision that brings together pedagogical, technical and regulatory dimensions.

Finally, one of the most innovative tools introduced in D4.3 is the Flexibility Table, designed to support the adaptation of games and educational activities to specific educational contexts. The Flexibility Table allows for the explicit linking of skills, learning objectives, teaching strategies, timelines, assessment methods, and local constraints. This tool facilitates mediation between theoretical frameworks and teaching practice, offering teachers and designers structured support for localising activities. The Flexibility Table makes design choices visible and facilitates the reuse and reconfiguration of resources, avoiding rigid or "pre-packaged" approaches.

4 What works in practice: evidence from the field

The considerations reported in this deliverable are based on evidence gathered during the pilot phase of the SuperCyberKids project, carried out as part of Work Package 6 (WP6) and documented in detail in the Pilot Report, which is attached to this deliverable.

The pilot phase represents a central step in the project, as it required translation of the conceptual and design principles of the SuperCyberKids ecosystem into real educational practices to be tested in diverse school contexts across Europe.

The pilots were not designed as controlled experiments but as situated implementations, integrated into the ordinary teaching activities of schools. This made it possible to observe the functioning of the ecosystem under real conditions characterised by organisational constraints, curricular differences, varying levels of digital competence among teachers, and uneven technological availability.

The evidence gathered is therefore particularly relevant for identifying transferable and sustainable good practices, rather than solutions that are only valid in hypothetical "ideal" contexts.

4.1 Structure and objectives of the pilot phase

Within Work Package 6, the pilot phase was divided into four localised case studies:

- Italy
- Estonia
- Germany
- EU pilot conducted in English.

All pilots took place between January and November 2025 and followed a common structure based on three main elements:

1) Activities aimed at training teachers, carried out online or in hybrid mode;
2) Classroom testing of specific modules from the SuperCyberKids ecosystem, selected on a voluntary basis;
3) Systematic collection of feedback through pre-training, post-training and post-pilot questionnaires, as well as post-pilot teacher interviews.

Each pilot was coordinated by a specific partner and adapted to the national or institutional context of reference, while maintaining a shared pedagogical core. This balance between a common structure and local adaptation was deliberately pursued to test the flexibility, robustness, and scalability of the ecosystem.

In all contexts, teacher training played an enabling role by introducing the SuperCyberKids learning framework, demonstrating lesson plans and use of the platform, and supporting teachers in reflecting on possible ways of integrating the tools and resources into their teaching practice.

Alongside teacher training and classroom experimentation, the pilot phase included specific actions to involve school leaders and recognise their strategic role in the adoption and curricular consolidation of cybersecurity education. School leaders were involved through the organisation of cross-cutting activities in the experimental contexts, which benefited from the involvement of the network of school leaders recruited by the project partner ESHA.

4.2 Implementation and adaptation models in the various pilot projects

Although they shared a basic structure, the pilot projects showed significant differences in their mode of implementation, offering a rich comparative perspective.

Specifically, the Italian pilot adopted a relatively standard model, based on a series of structured webinars dedicated to the learning framework, lesson plans, and teachers' online platform. The subsequent classroom trials involved many students. Given that trained teachers had the choice about whether to adopt the SuperCyberKids ecosystem in the classroom, this substantial take-up shows how a clear and well-structured teacher training programme can support large-scale adoption when accompanied by quality ready-to-use materials, including learning pathway designs.

The Estonian pilot followed a more flexible, bottom-up approach. After an open webinar, a select group of teachers chose to proceed with classroom testing, which was supported by the co-creation of localised lesson plans adapted to the national linguistic and curricular context. This pilot highlighted the importance of localising materials, teacher autonomy, and recognition mechanisms (such as certification) to encourage participation.

The German pilot combined online training and classroom experimentation, with a particular focus on involving school leaders. Although fewer classes were involved, the experience highlighted the

importance of structural factors, such as time constraints, school organisation, and difficulties in fostering take-up, all of which are crucial for the implementation of educational innovations.

Finally, the main objective of the EU-wide pilot, conducted entirely online and in English, was to test the scalability of the ecosystem in a single transnational context. The concise and flexible nature of the training sessions not only facilitated participation but also highlighted critical issues related to maintaining teacher involvement during the experimentation and feedback collection phases.

Taken together, these different implementation modes have shown how the same ecosystem can be adopted and reinterpreted in different ways, depending on institutional, cultural and organisational factors.

4.3 Participation scale and ecological validity

Overall, the SuperCyberKids pilot phase exceeded the project's initial quantitative objectives. Piloting activities involved 145 teachers in training activities and 480 pupils in classroom trials.

The diversity of the contexts involved reinforces the ecological soundness of the evidence collected. The analysed data reflect the complexity of real educational practices conducted in different contexts, rather than in simplified experimental conditions.

It is also important to note that the pilot phase focused primarily on school dynamics, with little direct involvement from parents or external stakeholders. This allowed for a more focused analysis of the role of teachers, students, and educational tools and resources for integration of cybersecurity into the curriculum.

Regarding school leaders, a total of 87 were reached through dedicated initiatives organised separately from the classroom pilots. The aim here was to promote an informed understanding of the educational, organisational, and curricular implications of integrating cybersecurity into schools.

Two specific initiatives for school heads played a central role:

- a guided discussion session at the ESHA conference held in Rome in October 2025, involving 67 school leaders from a wide variety of European and non-European countries. The activity, structured as a dialogue and supported by response collection tools (Mentimeter), explored the perceptions, priorities, and levels of experience of leaders regarding cybersecurity education;
- a dedicated workshop held in December 2025 in Istanbul, which involved school leaders and academics, who engaged in a focused discussion on the issues of cybersecurity for children, the institutional responsibilities of schools, and the conditions necessary for sustainable integration of cybersecurity education in the curriculum.

These initiatives did not have precise operational objectives but were designed to raise awareness and build capacity at the school governance level. They contributed to increasing school leaders' awareness of the educational relevance of cybersecurity and to clarifying the role of school leadership in supporting teachers and educational innovation. Moreover, these activities allowed the project to gather useful information on the organisational and political conditions that facilitate the adoption of new educational approaches.

The involvement of school leaders proved particularly significant, emphasising factors such as the availability of time, institutional recognition of activities, and alignment with school priorities. These all have a significant impact on the possibility of experimenting with and consolidating innovative practices.

In this sense, the activities aimed at school leaders served as a bridge between educational experimentation and policy recommendations, offering valuable insights into integrating cybersecurity into formal curricula and school development strategies.

4.4 Results from teachers' pre-training survey

This section presents an analysis of the pre-training survey conducted in the SuperCyberKids project. The aim is to describe the characteristics, perceptions, and practices of the teachers involved *prior to the training phase*, thereby providing a baseline for subsequent evaluation of training outcomes. The analysis was conducted as a part of the Final evaluation report of the SuperCyberKids project (R. 7.5.1)

The survey collected 121 valid responses from participating teachers in Estonia, Italy and Germany, as well as in other European schools participating online in the project (see table 1).

The questionnaire included closed and open-ended questions covering background characteristics, teaching contexts, familiarity with cybersecurity and gamification, current practices, and expectations.

Table 1: Responses by country of origin

Country	Number of respondents	Percentage of total
Estonia (EE)	45	37.2%
Italy (IT)	33	27.3%
Germany (DE)	23	19.0%
Other	20	16.5%
Total	**121**	**100%**

The school subject distribution (Table 2) highlights the **cross-curricular nature** of the teacher sample, with languages, mathematics/science, and ICT/digital skills accounting for around one-third of the total respondents.

Table 2: Which subject do you teach?

Subject	% of total respondents
ICT / Digital Skills	34.7%
Mathematics / Science	36.4%
Humanities (e.g. history, geography, social studies)	27.3%
Languages	37.2%
Arts	20.7%
Physical Education	9.9%
Other	0.0%

The country-level breakdown reveals **distinct disciplinary profiles** (Table 3). Estonian teachers are more strongly represented in ICT and science, while German respondents are mainly concentrated in humanities and languages. Italian teachers show a more balanced distribution, with a somewhat higher

concentration in languages. These differences point to the need for **flexible training resources** that can be effectively adapted to diverse subject areas across countries.

Table 3: Which subject do you teach (by country)?

Country	ICT / Digital Skills	Mathematics / Science	Humanities	Languages	Arts	Physical Education
Estonia (EE)	44.4%	46.7%	24.4%	24.4%	22.2%	8.9%
Italy (IT)	21.2%	24.2%	18.2%	33.3%	12.1%	6.1%
Germany (DE)	17.4% 30.4%	43.5% 56.5%	26.1%	17.4%		
Other countries	55.0%	40.0%	30.0%	50.0%	25.0%	10.0%

As to the breakdown of age range taught (Table 4), respondents reported teaching students aged **8–10 years (53.7%)** and **11–13 years (52.9%)**, indicating an even age-group spread across the project's target range of 8-13 years. In addition, more than one-third of respondents (36.4%) work with **mixed-age groups**, reflecting the presence of heterogeneous classroom settings and flexible teaching arrangements.

Table 4: Age range of students taught

Age range	% of total respondents
8–10 years	53.7%
11–13 years	52.9%
Mixed age groups	36.4%

Approaches to cybersecurity education (Table 5) vary substantially across countries. In **Estonia**, cybersecurity is most often addressed **both as a standalone subject and as an integrated part of other subjects (35.6%)**, whereas in **Italy** it is predominantly **integrated into other subjects (72.7%)**. **Germany** shows a more diversified pattern, with over half of respondents integrating cybersecurity into existing subjects, alongside smaller shares using standalone or combined approaches. In **other countries**, standalone provision is more common, suggesting diverse curricular strategies across contexts.

Table 5: Integration of cybersecurity education – by country

Country	Yes, integrated into other subjects	Yes, as a standalone subject	Both	No	I don't know
Estonia (EE)	22.2%	33.3%	35.6%	6.7%	2.2%
Italy (IT)	72.7%	0.0%	18.2%	0.0%	9.1%
Germany (DE)	56.5%	8.7%	17.4%	8.7%	8.7%
Other countries	35.0%	50.0%	10.0%	0.0%	5.0%

Respondents generally reported **moderate to high familiarity** with cybersecurity concepts (Table 6). The largest share indicated a **moderate level (44.3%)**, followed by **very familiar (37.4%)**. Perceived urgency of cybersecurity education notably tends towards the top of the scale, with the majority rating it

as **very or extremely urgent (67.8%)**. This reveals a clear gap between perceived importance and existing levels of familiarity.

Table 6: Familiarity with cybersecurity concepts and perceived urgency of cybersecurity education (% of total respondents, unified scale)

Scale level	Familiarity with cybersecurity (%)	Perceived urgency of cybersecurity education (%)
Not at all	0.0%	0.0%
Slightly	13.0%	4.1%
Moderately	44.3%	28.1%
Very	37.4%	29.8%
Extremely	5.2%	38.0%

Perceived urgency is high across all countries (Table 7), with **Germany (mean = 4.48)** and **Italy (mean = 4.45)** reporting the strongest sense of urgency. Respondents from **other countries** also show high urgency levels (4.35), while **Estonia** reports a comparatively lower, though still substantial, mean urgency score (3.31).

Table 7: Perceived urgency of cybersecurity education – by country

Country	Mean urgency[5]
Germany (DE)	**4.48**
Italy (IT)	**4.45**
Other countries	4.35
Estonia (EE)	3.31

While the importance of teaching cybersecurity is rated as **extremely high** by most respondents (86.0%), confidence in teaching it is more uneven (Table 8). Most respondents place their confidence at **moderate or very important levels**, but a non-negligible share reports **low confidence**, indicating a mismatch between perceived importance and self-assessed teaching readiness.

Table 8: Importance of teaching cybersecurity vs. confidence in teaching it

Scale level	Importance of teaching cybersecurity (%)	Confidence in teaching cybersecurity (%)
Not at all	0.0%	10.1%
Slightly	1.7%	10.9%
Moderately	0.0%	31.1%
Very	12.4%	36.1%
Extremely	86.0%	11.8%

[5] Urgency media (1 = not urgent at all; 5 = extremely urgent)

Levels of low confidence vary considerably across countries (Table 9). **Germany** shows the highest proportion of teachers with low confidence (43.5%), followed by **Estonia (20.0%)**. In contrast, **Italy (12.1%)** and respondents from **other countries (10.0%)** report lower shares, suggesting differences in prior exposure, training opportunities, or curricular support.

Table 9: Confidence in teaching cybersecurity (Not at all + Slightly)

Country	% low confidence
Germany (DE)	**43.5%**
Estonia (EE)	20.0%
Italy (IT)	12.1%
Other countries	10.0%

Regarding prior experience (Table 10), most respondents in surveyed countries have occasionally included cybersecurity topics in their teaching. Regular inclusion remains limited, particularly in Germany, where nearly 40% report never addressing these topics. Italy and Estonia show more frequent occasional or regular inclusion, while other countries display more even distribution across the experience scale.

Table 10: Inclusion of cybersecurity topics in lessons – by country (% within each country)

Country	No	Occasionally	Yes, regularly
Estonia (EE)	13.3%	66.7%	20.0%
Italy (IT)	9.1%	69.7%	21.2%
Germany (DE)	39.1%	52.2%	8.7%
Other countries	35.0%	30.0%	35.0%

Concerning the respondents' familiarity with gamification and game-based learning (Table 12), it is mostly **moderate (34.7%)** or **slight (29.8%)**, with a smaller share reporting high or extreme familiarity. This suggests that while game-based learning is widely known about, deeper expertise remains limited.

Table 11: How familiar are you with the concepts of gamification and using games in education?

Level of familiarity	% of respondents
Not familiar	14.0%
Slightly familiar	29.8%
Moderately familiar	34.7%
Very familiar	15.7%
Extremely familiar	5.8%
Total	**100%**

The majority of respondents use game-based approaches **occasionally (62.0%)**, while only a small proportion report **regular use (14.0%)**. Nearly one quarter do not use these at all, indicating significant potential for further development and support in this area.

Table 12: Do you use gamification and games in your teaching practices?

Response	% of respondents
Occasionally	62.0%
Yes, regularly	14.0%
No	24.0%
Total	**100%**

The open-ended responses about teaching strategies and tools currently used indicate that cybersecurity is most often addressed through **externally available online resources** rather than through purposely packaged and/or internally developed teaching materials. Teachers frequently refer to educational websites, institutional platforms, and publisher-provided digital resources, which are used as a primary source of content. In many cases, these resources are integrated in an ad hoc manner, depending on availability rather than on a predefined pedagogical framework.

Another recurring approach involves **discussion-based and explanatory practices**, such as oral explanations and guided classroom conversations about safe online behaviour. These activities tend to be informal and are often embedded within broader lessons rather than presented as dedicated instructional units. Overall, the responses suggest that cybersecurity education is commonly approached in a **fragmented and non-systematic way**, with limited use of structured tools or curricula specifically designed for this topic.

When asked about anticipated challenges in teaching cybersecurity, teachers commonly point to **student engagement and motivation** as a major concern. Many respondents note that students aged 8–13 often struggle to take cybersecurity seriously or fail to perceive online risks as real and relevant, which makes it difficult to sustain attention and interest. Closely related to this issue is the challenge of **age-appropriateness**: respondents emphasize the difficulty of translating complex and abstract cybersecurity concepts into language and examples that are meaningful and accessible to younger students.

A further challenge frequently mentioned concerns **teachers' own levels of expertise and confidence**. Several respondents expressed uncertainty about their ability to explain cybersecurity concepts clearly or to respond effectively to students' questions; this indicates a perceived gap between the importance of the topic and their preparedness to teach it. A smaller number of responses reflect a more **general sense of uncertainty**, with teachers indicating that they are not fully aware of the challenges they might face, partly due to the lack of clear guidance or established practices. In addition, some teachers refer to broader **communication and classroom management difficulties**, particularly when addressing sensitive or potentially alarming issues related to online behaviour.

Responses about the expectations and hoped-for outcomes of SuperCyberKids training reveal that teachers primarily hope the initiative will provide them with **practical, ready-to-use resources** that can be directly applied in classroom settings. Many respondents explicitly mention the need for concrete teaching materials, exercises, and activities that can support lessons conducted in computer labs or regular classrooms. This emphasis on applicability suggests a strong demand for resources that reduce preparation time and lower the barriers to integrating cybersecurity into everyday teaching practice.

Closely related to this, teachers frequently express the expectation of acquiring **new teaching strategies and methodological tools**. Rather than abstract knowledge, respondents highlight the value of learning how to effectively deliver cybersecurity content, adapt it to different age groups, and plan engaging lessons. This points to a desire for training that is strongly practice-oriented and pedagogically grounded.

Another recurring theme concerns **increased competence and confidence**. Several responses indicate that teachers hope the training will help them feel more knowledgeable and secure in addressing cybersecurity topics, enabling them to explain concepts more clearly and respond to students' questions with greater assurance. In this sense, the training is seen not only as a source of materials but also as a means of professional empowerment.

Finally, some respondents frame their expectations in terms of **positive outcomes for students**, emphasizing improved awareness, safer online behaviour, and tangible benefits for the class as a whole.

A smaller number of answers reflect uncertainty or limited expectations, either because respondents are not yet familiar with SuperCyberKids resources or because they find it difficult to articulate specific goals in advance.

4.5 Results from teachers' post-training survey

The post-training survey was designed to gather teachers' perceptions and opinions regarding the use of the SuperCyberKids platform. Comparison between pre- and post-training responses should also provide some indication of the perceived effectiveness of the training offered.

A total of 267 responses were collected through the post-training questionnaire. Out of these, 102 respondents completed the questionnaire in its entirety, corresponding to 38.2% of the total sample of teachers engaged in the SuperCyberKids initiative.

As to country of origin (Table 13), most respondents came from Estonia (12.4%), followed by Italy (10.9%) and Germany (7.5%). A small share of respondents selected "Other" or provided invalid entries. These results indicate geographically diverse participation.

Table 13: post-training survey response rates by country

Country	Responses (n)	Percentage (%)
Estonia (EE)	33	12.4%
Italy (IT)	29	10.9%
Germany (DE)	20	7.5%
Other	4	1.5%
Miscoded / invalid entries*	2	0.8%

Concerning the timing of participation in the SuperCyberKids training programme (Table 14), most respondents attended in April 2025 (32.4%), followed by November 2025 (23.5%), and March 2025 (15.7%). Smaller shares of participants attended in other months during 2025.

Table 14: Timing of participation in the training activities

Training date	Responses (n)	Percentage (%)
March 2025	16	15.7%
April 2025	33	32.4%
May 2025	6	5.9%
June 2025	1	1.0%
September 2025	3	2.9%
October 2025	2	2.0%
November 2025	24	23.5%

Regarding the timing of participation in the SuperCyberKids training programme (Table 15), most respondents attended the training in April 2025 (32.4%), followed by November 2025 (23.5%) and March 2025 (15.7%).

In terms of age range taught (table 15), 45.1% of respondents reported teaching students aged 8–10 years, while 37.3% indicated the 11–13 years age group. In addition, 34.3% reported teaching students of mixed ages. As respondents could select more than one option, these percentages are not mutually exclusive. Only completed questionnaires (N = 102) were considered in the analysis of this aspect.

Table 15: Age range of students taught

Age range	Responses (Yes)	Percentage (%)
8–10 years	46	45.1%
11–13 years	38	37.3%
Mixed age group	35	34.3%

In relation to subjects taught (table 16), respondents mainly reported teaching either Mathematics/Science or Languages (both 29.4%), followed by ICT/Digital Skills (25.5%) and Humanities (22.5%). Arts teaching was reported by 17.6% of respondents, while Physical Education accounted for a smaller share (7.8%). No respondents selected the "Other" category. As multiple answers were allowed, percentages are not mutually exclusive.

Table 16: Subjects taught

Subject taught	Responses (Yes)	Percentage (%)
Languages	30	29.4%
Mathematics / Science	30	29.4%
ICT / Digital Skills	26	25.5%
Humanities (e.g. History, Literature)	23	22.5%
Arts	18	17.6%
Physical Education	8	7.8%
Other	0	0.0%

Participants' response to the SuperCyberKids training and its potential downstream effectiveness were coupled in dual questions addressing overall rating of the programme in the first case, and preparedness to use SuperCyberKids resources after training in the second. (table 17). Here, generally positive results were achieved. Overall evaluation of the training was favourable, with an average score of 7.76 on a 1–10 scale and a median value of 8. While some variability is observed, the results suggest broadly positive acceptance of the programme.. Secondly, respondents reported a high level of perceived preparedness to incorporate SuperCyberKids resources in their teaching (mean = 4.06 on a 1–5 scale).

Table 17: overall rating of SuperCyberKids training and preparedness to use SuperCyberKids resources after training

Indicator	Valid responses (n)	Mean	Median	Std. deviation
Overall rating of the SuperCyberKids training (1–10)	72	7.76	8	1.86
Preparedness to use SuperCyberKids resources in your teaching after being trained on the use of SuperCyberKids resources (1–5)	86	4.06	4	0.83

Broken down by country, overall satisfaction with the SuperCyberKids training programme is generally high across countries (table 18). Italian respondents report the highest satisfaction level (mean = 8.63), followed by Estonian (7.85) and German teachers (7.25). Respondents from other countries show a lower mean score (6.50), although this result is based on a very small number of results. These findings suggest

some cross-country variation in perceived satisfaction, which may reflect differences in training delivery, expectations, or local educational contexts.

Table 18: training programme satisfaction by country

Country	Responses (n)	Mean satisfaction (1–10)
Italy (IT)	27	8.63
Estonia (EE)	33	7.85
Germany (DE)	20	7.25
Other countries	4	6.50

Regarding the open question on what specific contents of the training programme were found most useful, respondents most frequently indicated the practical and concrete components of the training. Specifically, interactive activities and the game-based approach were highly rated for their capacity to engage students and to translate abstract cybersecurity concepts into accessible and age-appropriate learning experiences.

Several respondents appreciated the training's focus on real-life digital risks, such as online safety and responsible behaviour, noting that these topics are highly relevant to students, especially those with special education needs. The availability of ready-to-use materials and examples that could be directly integrated into classroom activities was also seen as a key strength of the training programme.

The overall picture that emerged was that the most useful aspects trainees saw in the training were those that combined **practical applicability, clarity of content, and alignment with everyday teaching needs**.

Potential improvements in the training programme that respondents suggested were better content alignment with their specific teaching context and more appropriate difficulty levels for students' age and prior knowledge.

Several comments pointed out that, for some student groups, the activities were either potentially too basic or not sufficiently differentiated, indicating the need for more training guidance in selecting the appropriate level or module.

Another recurring suggestion concerned the structure and delivery of the training. Some respondents proposed adjusting the duration and pacing of sessions, as well as providing clearer instructions, particularly for the game-based components, which were sometimes perceived as being not particularly intuitive.

Finally, some respondents recommended increasing focus on digital and computer-based activities in training and reducing emphasis on paper-based materials to better match with students' preferences and everyday classroom practices. Overall, suggested improvements to the training resources focused on **enhancing clarity, adaptability, and practical applicability**.

The final question in the survey called on respondents to state whether they would recommend the training programme to other teachers and if so, why. This was essentially an attempt to measure perceived effectiveness of the SuperCyberKids training programme as enacted with the different teacher cohorts involved. Overall, respondents expressed a positive position: the programme was described as useful, relevant, and well aligned with current educational needs in the field of digital safety and cybersecurity. At the same time, several respondents noted that the training programme would benefit from better

adaptation to student age and prior knowledge level, as well as clearer structuring and timing of activities. Despite this, the training programme was generally perceived as valuable preparation for addressing cybersecurity topics in the classroom via SuperCyberKids.

4.6 Results from teachers' post pilot survey

In addition to the pre- and post-training surveys completed by teachers who underwent the SuperCyberKids training programme, a further questionnaire was submitted to teachers who had enacted classroom pilot activities. A total of 12 questionnaire responses were collected after completion of the pilots, which were held to test SuperCyberKids tools and resources. Responses came mostly from Italy (9), together with one each from Germany, Estonia and Spain (table 19 below).

Table 19: teachers' post pilot survey response rates

Country	Responses
Italy	9
Germany	1
Estonia	1
Spain	1
Total	**12**

The teachers who completed the survey engaged a total of 438 students in classroom activities, with an average of approximately 40 students per teacher (based on 11 valid responses).

The majority of teachers indicated that their students were primarily in the **8–10 age range** (6 responses), followed by the **11–13 age range** (5 responses), with 2 cases involving **mixed-age groups**.

The survey respondents primarily taught ICT/Digital Skills and Humanities (4 teachers each), followed by Mathematics/Science (3 teachers). Other subjects taught include Estonian language, Mathematics, Civic and Natural Sciences, Arts and Technical Education, and Music. One respondent is a preschool teacher.

When asked about student reaction to the enacted SuperCyberKids experience, the majority of responding teachers reported that most students reacted **very enthusiastically and remained engaged** throughout the activities (9 responses). A smaller group reported **intermittent engagement** (2 responses), while no cases of neutral, disinterested, or disengaged behaviour were reported.

Table 20: Teacher-reported student response to the SuperCyberKids experience

Response option	Count
Very enthusiastic and engaged throughout	**9**
Engaged at times but lost interest occasionally	**2**
Neutral, neither particularly engaged nor disengaged	0
Disinterested, found it difficult to focus	0
Actively disengaged and uninterested	0

Other	0

As illustrated in Figure 1 below, respondents rated the effectiveness of SuperCyberKids resources very positively, with an average score of 4.6 out of 5, indicating a very positive perceived overall value of the resources.

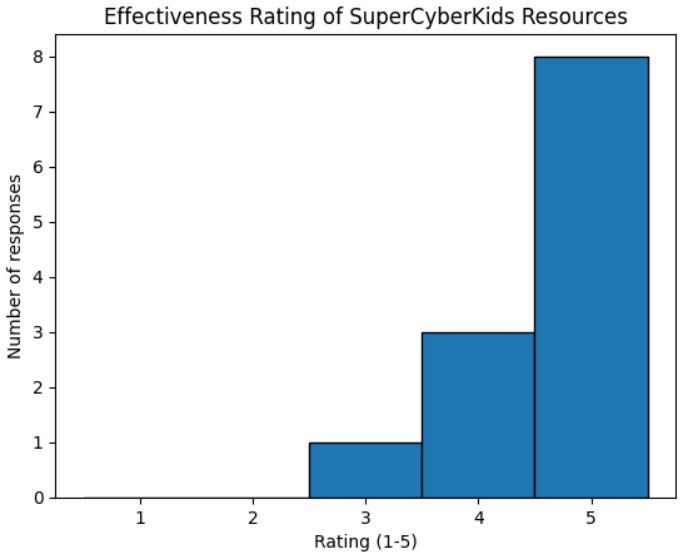

Figure 1: Teacher rating of SuperCyberKids resource effectiveness

The resource types considered most useful (table 21) were Games and Lesson Plans (both with nine mentions), followed by pdfs, presentation Slides, and website/external links. Videos were selected less frequently, and no respondents indicated "Other resources".

Table 21: resource types considered most useful in the SuperCyberKids experience

Resource type	Count (YES)
Games	**9**
Lesson Plans	**9**
PDFs	**5**
Presentation Slides	**4**
Website / External Links	**4**
Videos	**3**
Other	**0**

Regarding perceived enhancement in students' understanding of cybersecurity (Figure 2), ratings were strongly positive. Indeed, on a scale of five (1 = Not at all, 5 = Extremely) respondents assigned scores of 4 or 5, and no scores below 3.

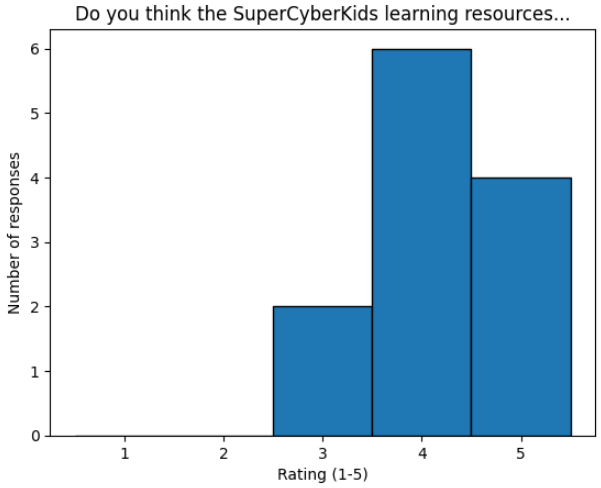

Figure 2: teachers' perception of enhancement in student understanding of cybersecurity

The most engaging component for teachers was **games**, selected by nine respondents, followed by **lesson plans** and **web links**. More traditional materials such as **pdfs**, **slides**, and **videos** were considered less engaging overall.

Table 22: Type of SuperCyberKids learning resource rated by engagement

Engaging aspect	Count (YES)
Games	9
Lesson Plans	5
Website / External Links	4
Presentation Slides	3
Videos	2
PDFs	1

4.7 Challenges and recommendations expressed by teachers

Respondents mentioned only a limited number of difficulties while using SuperCyberKids ecosystem. The main challenges mentioned concerned adapting the activities to younger children, understanding gameplay and game instructions in the initial phase of use, managing some technical aspects of the online environment, and dealing with slower pacing in larger classes. A **few teachers** also noted that **they needed to familiarise themselves more thoroughly with certain cybersecurity topics before teaching them**. At the same time, a substantial number of respondents explicitly stated that they experienced no particular challenges.

When asked whether they would recommend the resources to colleagues, the responses were overwhelmingly positive. Teachers generally appreciated the usefulness and relevance of the materials, noting that these helped simplify lesson planning, increase student motivation, and promote awareness

of cybersecurity—an increasingly important subject. **Several respondents highlighted that the resources are engaging and well aligned with educational objectives**.

A few pointed out that, while they would recommend the materials, the level of difficulty needs to **be better calibrated to different age groups**, as some activities were perceived as too basic or too challenging, depending on the class.

Responding teachers offered several constructive suggestions for making improvements. A number of them proposed further adapting the materials to different age ranges, even beyond the SuperCyberKids 8-13 target range. For example, some suggested **simplifying content for children aged 8–10**, providing **more advanced content for students over 13**, or creating dedicated resources for children under eight. Other suggestions included expanding the range of topics covered, **increasing hands-on or laboratory-style activities, reducing reliance on paper-based exercises in favour of digital ones**, improving game usability and clarity in game navigation, and **offering mechanisms for tracking student progress**. Some teachers stated that they considered the resources already complete and well-structured and therefore offered no further suggestions.

As to future use of SuperCyberKids ecosystem, teachers expressed their intention to continue use beyond the pilot phase. Teachers' willingness to reuse the resources and to recommend them to colleagues not only reflects satisfaction with the materials, but also hints at broader acceptance of cybersecurity as a relevant and enduring component of the educational curriculum. In this sense, the SuperCyberKids project appears to contribute to a shift from ad hoc approaches towards more stable and routinised forms of cybersecurity education.

While commitment appears strong at the level of individual teachers and schools involved in activities, broader institutional anchoring—such as clearer links to national curricula or formal educational guidelines—remains limited and could enhance legitimacy and uptake. Finally, continued investment in teacher training and follow-up support appears necessary to consolidate confidence and ensure that cybersecurity education becomes a stable and routine component of teaching. While the SuperCyberKids project provides clear evidence of strengthened commitment to cybersecurity education among teachers, addressing these gaps will be essential to support wider diffusion and long-term curricular integration.

5 Evidence-based good practices

This section presents an initial set of evidence-based good practices that emerged from analysis of classroom piloting activities and from semi-structured interviews conducted with teachers who used SuperCyberKids resources in real school contexts. The aim is to highlight not only the 'pros and cons' but, above all, to pinpoint the conditions of effectiveness, adaptations, constraints, and teaching orchestration strategies. The good practices are organised into three areas: teaching practices, educational design practices, and organisational practices.

5.1 Good Teaching Practices

In SuperCyberKids, teaching practices chiefly revolve around adoption of game-based activities for engaging young learners in cybersecurity education - with all the complexities that process can involve. Key to this endeavour is teacher's guidance and strategies for transforming play into learning: orchestration of activities, debriefing, prevention of superficial game use, differentiation by age, and the pedagogically safe management of sensitive issues.

The following table systematically lists the good practices that emerged.

ID	*Good practice*	*Rationale*	*Practical guidelines*	*Evidence/quotes from the interviews*
GP-T1	Teacher orchestration and "direction" of the game (before, during and after)	The interviews show that the educational effectiveness of the game depends strongly on how it is "framed" by the teacher: preparation (objectives and key vocabulary), management of the activity (turn-taking, pauses, clarifications), and post-activity reflection.	• Before the game: state 1–2 objectives and 3 key words (minimum vocabulary). • During: introduce check-in pauses (checkpoints) to ask, "What choice would you make and why?" • After: a short guided debrief (see GP-T2 immediately below) to turn the play experience into transferable learning.	"Approaching children in a practical way… giving practical examples… [is] engaging."
GP-T2	Structured debriefing as a learning "multiplier"	Several teachers report that guided discussion after each "world" /phase of the game consolidates concepts, brings out prior experiences, and supports connections with everyday life.	• What happened? (shared reconstruction: 2–3 events/decisions). • Why does it matter? (risk/protective strategy). • What would I do in real life? (1 concrete example per student or in small groups).	"We discussed everything with kids after each world and that helped a lot."
GP-T3	Prevent "superficial" use (click-through) in micro-tasks and roles	The interviews highlight a recurring tension: the game increases engagement, but it can lead to interaction focused on progression (or secondary elements) rather than on the core content.	• Integrate a short worksheet/mission (2–3 questions) to be completed during gameplay. • Assign roles: navigator (plays), observer (notes choices and messages), spokesperson (reports during the debrief). • Set a rule: "You do not move to the next level without answering one comprehension question".	"Some learn more about cyber, others focus on collecting items in the game."
GP-T4	Age differentiation and language adaptation (8–9 vs 10–11 vs 12–13)	Teachers confirm that younger pupils need language mediation and simplification; the age threshold of 9 is explicitly mentioned as a practical reference point for greater autonomy.	• Ages 8–9: more concrete examples, short sentences, visual support; greater teacher guidance. • Ages 10–11: increasing autonomy; application tasks (rules, checklists). • Ages 12–13: discussion of more complex cases (privacy, disinformation, abuse), with greater responsibility.	"They're a bit small... in some cases I've adapted them... but in my opinion, from the age of 9..."
GP-T5	Pedagogical safety on sensitive topics: gradualness and "responsible lightness"	When addressing risks related to grooming and inappropriate content, the interviews indicate the need for protective communication: helping pupils understand the risk without making age-inappropriate details explicit. Using strategies such as simulations or roleplays can be beneficial.	• Use metaphors, protected scenarios, and "warning signs" (red flags) rather than explicit details. • Adopt controlled role-play (who would you ask for help? what would you say? to whom?). • Always close with protective strategies and help channels (trusted adult).	Evidence: teachers requested that sensitive topics be addressed with caution and gradualness, keeping the focus on protective strategies. (Source: Interview Summary – piloting teachers)

5.2 Good Educational Design Practices

Educational design practices concern the quality and usability of the lesson-plans and the gamification platform, including onboarding and usability, technical robustness, alignment between game mechanics and learning objectives, modularity of materials, and the inclusion of lightweight assessment. The following table summarises the design recommendations that emerged from the interviews.

ID	*Good practice*	*Rationale*	*Practical guidelines*	*Evidence/quotes from the interviews*
GP-D1	Accessibility and usability: make "how to use the platform" visible	Teacher feedback (also via email) shows initial barriers: the platform UI is perceived as not very user-friendly. Difficulty understanding that the homepage map is "draggable" without an explicit hint. Contextual help pop-ups seen as intrusive, PDFs as not scroll-friendly.	• Micro-onboarding (10–20 seconds) with contextual hints (e.g., "you can drag the map"). • Non-invasive help (enable/disable). • PDF materials in a genuinely usable format (scrolling, mobile/tablet).	"I realised the hand meant that I could drag the 'map' around… it might be a barrier… a simple pop up…"
GP-D2	Technical robustness and session continuity: pay attention to reduce crashes, lag, and recovery issues	Crashes and bugs are reported (e.g., objects that cannot be removed, lag). These issues directly affect classroom adoption and the ability to maintain teaching orchestration.	• Automatic session saving and resuming. • The games and the platform should clearly signal the connection or loading status. • Testing on typical school devices (older PCs, tablets, unstable networks).	Reports of crashes/bugs/lag and the need for recovery.
GP-D3	Game mechanics and educational goals: avoid letting play mechanics "override" content engagement	A teacher notes that students tend to focus on elements such as "pets" or collecting items, reducing the students' attention on cybersecurity topics.	• Make the link between a mechanic and a concept explicit (brief educational feedback after a choice). • Provide in-game micro-tasks oriented to content (not only collecting). • If "decorative" elements are present, provide them with a minimal educational function (e.g., hints, reminders).	"The kids… focused on getting as many pets as possible."
GP-D4	Integrate ready-to-use, compressible materials: modularity and reuse	Teachers appreciate the structure and accessibility of the materials but report time constraints and a need for adaptation.	• Each unit should have a base version (45–60 min) and an extended version (90–120 min). • A structure of reorderable blocks: introduction – game – consolidation – check. • Downloadable and reusable resources (slides, worksheets, cards, checklists).	"The resources are clear and well organised, and they are accessible."
GP-D5	Integrate lightweight assessment: quizzes and observation tools	A recurring request emerges in the interviews: a quiz (or similar) to check what has been learned, and the possibility for teachers to monitor progress.	• Short pre/post quiz (5–8 items), reusable. • Observation checklist (3 indicators): participation, understanding of risk, correct strategy. • Minimal class report (exportable) to support documentation and reflection.	"There should be a quiz… at the end to check what the kids have learned."

5.3 Good Organizational Practices

Organisational practices concern the conditions that make adoption sustainable over time. Integration within curriculum constraints and school timetables, reuse and sharing among teachers, and cross-curricular positioning are typical examples. The following table reports the organisational good practices that emerged from the interviews.

ID	*Good practice*	*Rationale*	*Practical guidelines*	*Evidence / quotes from the interviews*
GP-O1	Adopt "realistic" planning: integrate within curriculum constraints and school timetables	Teachers report strong constraints due to curricula and school time; they suggest that a structured module has greater impact, but it must be sustainable and plannable.	• Prefer short, repeatable units (cycles) over long isolated interventions. • Provide an adoption roadmap: 1 pilot unit → 2 units → short module.	"We are also very constrained by schedules..."
GP-O2	Facilitate reuse and sharing among teachers: materials that can be stored and transferred	A teacher highlights the practice of saving and reusing materials, also sharing them with STEM/technology colleagues; this is an enabling factor for scalability and continuity of use.	• Create a school (or network) repository with adapted materials, implementation notes, and age variants. • Enable the continuous integration of the ecosystem through the sharing of new materials by teachers and other participants in the community of practice. • Minimum sharing standard, like objectives, duration, prerequisites, adaptations made.	"I saved the content... to reuse it... and share it on... to colleagues..."
GP-O3	Cross-curricular positioning: civic education + technology + subjects	The teacher identifies "natural" placements in technology and civic education, as well as concrete cross-curricular links anchored to news/everyday life.	• Define a map of links: civic education (behaviours), technology (security and devices), first/foreign languages (comprehension and communication), history/geography (citizenship and context). • Use everyday "triggers" (news, real episodes) as hooks to revisit concepts.	

5.4 Summary

The interviews converge on the idea that the educational value of games is not automatic but depends on the teacher's orchestration: setting objectives, guiding interaction to prevent "surface-level" use (focused only on passing levels or collecting items), and concluding with a structured debriefing that turns the play experience into transferable concepts and behaviours. Moreover, teachers highlighted the need to differentiate language and depth by age (8–13) and address the more sensitive topics gradually and with "responsible lightness", keeping the focus on protective strategies.

Teachers point out that classroom adoption requires an accessible platform (clear onboarding, explicit affordances, and usable materials), technical robustness (stability and session recovery), and coherence with educational objectives (game mechanics should not override the content). They also consider it crucial to provide ready-to-use materials that are ready to use but can be compressed and reused, along

with lightweight assessment tools (pre/post quizzes and checklists) that make learning outcomes and progress visible.

Finally, the interviews indicate that sustainability depends on realistic integration within curriculum constraints and school timetables, on reuse and sharing among teachers (school/network repositories), on cross-curricular positioning (civic education, technology, and links with other subjects), and also on everyday "triggers," such as news or real cases.

6 Recommendations for key stakeholders

6.1 Recommendations for teachers and schools

The evidence gathered from project activities confirms and "grounds" a point already central to the points made in Deliverable D3.1: integration of cybersecurity in the curriculum should be managed as a process of educational orchestration carefully combining objectives, content, methods and assessment in a way that is sustainable over time and compatible with school constraints.

SuperCyberKids training and piloting data show a strong demand for ready-to-use materials that reduce the preparation burden and offer teachers concrete guidance on how to "turn play into learning". Piloting results also indicate very high levels of engagement and a perception of high effectiveness (very positive average ratings), with a clear preference for games and lesson plans as the most useful and engaging resources.

A first recommendation is to **design game-based activities as structured pathways**, where the game is a core - but not all-embracing - part of learning. Good practices emerging from the interviews indicate that effectiveness depends decisively on how the teacher frames the game (before, during and after play) through micro-objectives, a minimum shared vocabulary, reflection phases, and moments of clarification.

In this sense, structured debriefing is a key step acting as a "multiplier" of learning: guided reconstruction of what happened and why it matters is essential for transferring what has been discussed to real-life cases. This evidence updates what was outlined in Deliverable D3.1 in a highly operational way; it is not enough to state that cybersecurity should be integrated in the curriculum. Teachers also need concrete guidance to make the experience transferable and assessable, without threatening sustainability.

In this light, the SuperCyberKids ecosystem responds well because it was designed as a modular and graded structure. The platform features a map of 18 modules organised by focus and level (areas: technical, social, integrated; levels from basic to advanced). Each module is accompanied by four lesson plans (Introduction, Game-Based Learning, Consolidation, and Assessment), which can be printed and reused, allowing teachers to maintain control over teaching without "delegating" learning to the game.

In addition, the platform provides access to resources, allows courses to be managed, and features gamification elements (points/badges) for teachers. It also includes useful features such as module navigation, an updatable repository of materials ("Community items"), search functionality, as well as special features that support educational use. The presence of a feedback form at the end of each module enables the collection of "light" but continuous evidence on adoption, facilitating iterative improvement and teaching accountability.

A second recommendation concerns **differentiation by age and prerequisites**. The questionnaire responses, including both ratings and qualitative comments, indicate a desire to better calibrate difficulty and progression. Some activities may be perceived as too simple or too complex depending on the class, and there is demand for materials that are more differentiated by age (8–10 vs 11–13, and even beyond

the target age group). Operationally, this translates into an adoption criterion: teachers should carefully choose the module to adopt and how materials are to be used (monitored, in groups, individually, etc.) based on pupils' age, level of digital skills, context (laboratory or classroom) and time available, adapting the lesson plan without distorting it. Furthermore, translations into first language would be useful, especially for pupils.

Finally, regarding assessment (another axis of Deliverable D3.1), the evidence suggests focusing on integrated and formative assessment, in line with the competence-based approach. A flexible approach can prevent assessment from becoming an organisational obstacle. This involves combining (depending on teacher preferences) classroom observation, assignments and artefacts, and (where possible) pre/post checks or micro-tests.

Table 23: Recommendations for teachers and schools

Level	Focus	Recommendations	Implementation tips
Teacher	Learning design	Plan the activity as a before–during–after sequence (introduce → play → consolidate).	Use a short problem scenario to open; close with a 5–10 minutes debriefing and a takeaway rule.
	Concept clarity	Make a minimum shared vocabulary explicit (key terms and concepts).	Provide 5–8 keywords on the board/slide; ask pupils to use them when explaining choices.
	Facilitation	Frame play with micro-objectives and moments of clarification (avoid "clicking through").	Use guiding questions during play; pause at key moments to connect actions to risks/protections.
	Debriefing	Use structured debriefing as a learning multiplier (transfer to real-life cases).	Guided reconstruction: what happened, why it matters, and what rule/strategy applies outside the game.
	Differentiation	Adapt scaffolding, organisation and duration to age/prerequisites (8–10 vs 11–13 and beyond).	Pairs/teams and closer monitoring for younger pupils; more autonomy and discussion for older pupils.
	Assessment (light)	Use integrated, formative assessment without increasing workload.	Observation, short reflections, artefacts/assignments; micro pre/post checks when feasible.
School	Sustainability	Ensure realistic time allocation and continuity over the year (repeatable units).	Adopt short modules (45–60') and optional extensions (90–120'); create a simple yearly plan.
	Coordination	Support reuse and adaptation through teacher collaboration and shared resources.	Maintain a shared repository with notes on duration, prerequisites and adaptations.
	Curricular integration	Formalise cross-curricular anchoring (e.g., civic education + links to other subjects).	Map modules to curriculum topics; use real news/events as triggers for discussion.
	Ecosystem use	Leverage platform features to reduce burden and support continuous improvement.	Use lesson plans (Intro / GBL / Consolidation / Assessment), "Community items", search, and module feedback forms; consider points/badges where appropriate.
	Classroom logistics	Provide organisational routines for devices, turn-taking and technical contingencies.	Prepare device rotation rules; test connectivity; have offline/printable backup activities.

Table 24: Quick checklist for teachers and schools

DOs	DON'Ts
• Always close with a short, guided debriefing to connect play to real-life cases. • Make key concepts explicit (minimum vocabulary + micro-objectives) before and during play. • Keep assessment light and formative (observation/artefacts/micro checks) to stay sustainable.	• Don't treat the game as all-embracing: without framing, engagement may not translate into learning. • Don't apply a "one-size-fits-all" difficulty level: calibrate by age, prerequisites, context and time.

6.2 Recommendations for parents and families

Piloting results confirm that, especially for children aged 8–13, cybersecurity education should be located at the boundary between formal and informal contexts, e.g., school and home. Moreover, evidence suggests that the motivation generated by game-based activities tends to "spill over" outside the classroom, as many children continue or revisit the experience at home. This amplifies educational opportunities but also raises concerns related to screen time and children's independent management of digital activities.

For this reason, parents should not be considered merely as "technical users" within the ecosystem but as educational allies who can reinforce safe behaviours, ensure consistent messaging, and support age-appropriate discussions about real risks.

In line with the institutional and school policy dimension highlighted in Deliverable D3.1, parental involvement should therefore be structured through clear, proactive communication. This is precisely what the SuperCyberKids ecosystem offers.

Specifically, the SuperCyberKids ecosystem states why cybersecurity education is relevant for children's digital development and what outcomes are expected from the learning process.

The enactment package described in Deliverable D5.2 further supports this approach by framing the introduction of SuperCyberKids to parents as a responsibility of those coordinating adoption at the institutional level. In addition, whenever assessment or data collection tools are used (even minimal ones), a transparent, respectful and reversible approach is recommended, including options for anonymisation and informed consent/withdrawal.

The ecosystem facilitates this recommendation by making the school experience more explainable and transparent. Lesson plans and accompanying metadata clarify the stages of the pathway (introduction–play–consolidation–assessment) and help schools communicate that the intervention is not "just playing" but a structured and intentional educational process. Finally, debriefing activities and links to real-life cases support transfer to the home in a way that avoids anxiety-provoking or moralistic tones, and instead focuses on choices, consequences, and practical strategies.

Table 25: Recommendations for parents and families

Level	Focus	Recommendations	Implementation tips
School / Institutional Level	Communication & trust	Provide clear, proactive communication to parents about the pathway, its goals, and expected outcomes.	Use a short parent info sheet + FAQ: "what it is", "why it matters", "what children will do", "what you can do at home".
	Explainability of the pathway	Make the learning pathway visible (introduction–play–consolidation–assessment) and communicate its objectives and rationale.	Share a one-page "roadmap" per module; reference the lesson plans and key concepts addressed.
	Data, consent & transparency	Manage any data/consents with a transparent, respectful and reversible approach.	Consent/withdrawal options; minimise data; anonymise where possible; communicate what is collected and why.
	Home–school continuity	Encourage consistent messaging and continuity between classroom and home.	Suggest short discussion prompts after modules (e.g., "What would you do if…?" scenarios).
Parents / Families	Educational ally role	Reinforce safe behaviours and consistent messaging without turning it into policing.	Use brief, recurring conversations; ask children to explain rules/strategies in their own words.
	Screen time & autonomy	Support routines for time and supervision appropriate to age.	Agree on time limits; prefer shared use for younger children; check-in moments rather than constant monitoring.
	Real-life transfer	Use debriefing-style dialogue to connect play to real risks and practical strategies.	Focus on choices, consequences, protective actions (privacy, passwords, reporting, asking for help).
	Tone and emotional safety	Avoid anxiety-provoking or moralistic framing; emphasise agency and help-seeking.	Normalise "asking an adult"; discuss "what to do next" rather than "what you did wrong".

Table 26: Quick checklist for parents and families

DO	DON'T
• Communicate early and clearly what the learning pathway is (goals, stages, expected outcomes) and how data/consents are to be handled. • Promote home conversations that focus on strategies and decision-making (choices, consequences, protective actions) and not fear or blame.	• Don't leave parental involvement to informal word-of-mouth. Lack of clarity increases mistrust and reduces continuity at home. • Don't treat assessment/data collection as a purely technical matter. It is fundamental to ensure transparency, minimal burden, and reversible consent.

6.3 Recommendations for educational game designers and developers

In Deliverable D4.3, we strongly support the idea that a learning game should be conceived as a transmedia artefact. This means that the game itself represents the tentpole component, but its educational effectiveness depends heavily on the presence of related resources (e.g., lesson plans, quizzes, discussion prompts, guides, and community spaces) that enable reuse and adaptation. This framing is particularly relevant in cybersecurity education for children aged 8–13, where learning outcomes depend not only on engagement but on the possibility to make concepts explicit, to connect them with real-life situations, and to sustain adoption under everyday school constraints.

According to the evidence gathered during piloting, the role of supporting materials becomes even more central. These resources are not simply a useful but optional "kit". They function as an adoption infrastructure that allows teachers to orchestrate activities without friction, that ensures operational continuity, and maintains the centrality of cybersecurity content. In other words, the value of supporting materials and platform features can be measured in their ability to:

(i) make it immediately clear "how to use" the ecosystem
(ii) prevent interruptions and session losses
(iii) prevent play-oriented game mechanics from prevailing over content engagement
(iv) offer ready-to-use but compressible and reusable materials
(v) integrate forms of light and sustainable assessment.

This view directly updates and strengthens the recommendations in Deliverable D4.3: in real classroom conditions, adoption is not only a matter of content quality, but also of reducing uncertainty and ensuring lesson continuity.

A first operational implication concerns the community and repository dimension. Deliverable D4.3 already highlights the community as an enabling factor, ensuring that games are sourced, adopted, and supported over time. It also frames the SuperCyberKids platform as a space set up for sharing and reuse. Piloting evidence reinforces this direction but specifies a stricter requirement: the community space should not operate as a mere "showcase" of materials, but as a practical repository for teaching work—resources must be quickly filterable, selectable and reusable, with a brief, concise description that reduces implementation uncertainty. The "Community Items" area on the SuperCyberKids platform - designed as a shared repository based on cards (descriptions, associated skills, resource types, ratings, and personal playlists) - is consistent with this approach. However, evidence indicates that quality and usability depend on contextualisation. Effective sharing requires context for use, not just files or links. For designers and developers, this translates into the need for a standard set of metadata and implementation notes (e.g., actual duration, prerequisites, adaptations made, tested age group, technical difficulties encountered and solutions adopted). This directly supports reuse and transferability—two criteria that teachers consistently associate with sustainability.

A second implication concerns guides, playthroughs and onboarding. Deliverable D4.3 recommends video playthroughs and guides to support teachers who may not be comfortable completing a game, avoiding frustration and abandonment, especially in the presence of progression/unlock mechanics. Piloting activities confirm this point but expand it substantially. Initial barriers are not only about "not knowing what to do", but also about difficulty grasping essential affordances (e.g., the platform homepage map being draggable), the perception of intrusive help, and the poor usability of some PDFs. Moreover, crashes and lag interrupt learning orchestration, turning a technical problem into a classroom management problem and ultimately threatening attainment of the educational objective. The priority for designers and developers therefore is to implement contextual micro-onboarding and a help system that does not interrupt flow. At the same time, it is necessary to ensure session continuity (automatic saving, resuming, clear loading/connection indicators, and testing on typical school devices and unstable networks). These requirements are expressed in good practices GP-D1 and GP-D2, and make the Deliverable D4.3 recommendation more stringent: guides and playthroughs should protect the lesson from friction and interruption without compromising game activity.

A third implication concerns ready-to-use lesson plans and materials. Deliverable D4.3 links lesson plans to the outcomes and competency statements of the project's learning framework and proposes a reference structure (e.g., Presentation, Practice, Production pattern), emphasising the importance of stating context of use and required resources. The results of piloting activities add a recurring, highly operational demand: teachers appreciate clear and well-organised materials, but face time constraints and

a strong need for adaptation. This implies that materials must be (a)ready-to-use and compressible, offering a basic version (45–60 minutes) and an extended version (90–120 minutes and (b) structured in reorderable blocks (introduction, game, consolidation, check) and downloadable/reusable materials like slides, worksheets, cards, checklists. For designers, this means designing the lesson plan as a "modular object", where each block states the minimum target and what is lost if it is cut, so that compression does not distort the unit. For developers, this means ensuring formats are genuinely usable in educational contexts (scrolling, tablet/mobile viewing, fast access), because poor usability of materials becomes a concrete barrier to adoption. The platform can further support modularity if it makes the coexistence of basic/extended variants natural and facilitates selection, download, and playlist insertion.

Finally, the insights collected through the piloting activities highlight a tension typical of learning games that directly updates Deliverable D4.3: during gameplay, engagement can shift to secondary elements, reducing focus on cybersecurity constructs. Beyond providing supporting materials, gameplay and learning experience design must make the connection between action/mechanics and concept explicit, integrating educational micro-feedback and content-oriented micro-tasks. If decorative elements such as collectables are a feature, ideally they should have at least a minimal educational function (hints, reminders, signals). In parallel, teachers request simple tools to check what has been learnt and, where possible, monitor progress. This does not mean complex evaluation systems, but rather light and sustainable assessment, such as short pre- and post- quizzes and observational checklists. This need is formalised in Good Practice GP-D5, and complements the supporting materials framework already described in Deliverable D4.3. For developers, it implies making assessment tools easily accessible and reusable as platform objects. For designers, it requires aligning these with the 8–13 age group and lesson time constraints, so that assessment concludes the teaching cycle, making learning visible and discussable rather than burdening the experience.

Table 27: Recommendations for designers and developers

Area	Focus	Recommendations	Implementation tips
Community / Repository	Reusability with context	Treat the community space as a **teaching-work repository**, not a showcase: resources must be filterable, selectable and reusable with minimal uncertainty.	Require short "context notes" for shared resources (tested age, duration, prerequisites, adaptations, what worked).
	Metadata standard	Define a minimal **metadata + implementation notes** structure to support transferability and sustainability.	Include: actual duration, prerequisites, tested age group, adaptations made, technical issues encountered and solutions adopted.
	Decision support	Support reuse decisions through simple signals (ratings, tags, resource types, skills) and teacher workflows.	Card-based items with tags + ratings; personal playlists; "most reused/most adapted" indicators.
Guides / Playthroughs	Avoid frustration	Provide guides/playthroughs to reduce abandonment, especially with progression/unlock mechanics, without replacing play.	Teacher-facing "what happens next" walkthrough; common pitfalls; "where pupils may get stuck" notes.
Onboarding / Help	Non-invasive support	Implement **contextual micro-onboarding** and help that does not interrupt the flow (short, repeatable, disable/able).	Tiny hints for hidden affordances (e.g., draggable map); side-panel help; avoid blocking pop-ups.
Session continuity	Recovery & resilience	Protect lesson continuity: ensure autosave/resume and clear status indicators; design for school networks/devices.	Resume-from-last-state; explicit loading/connection status; smooth handling of lag/crashes; quick restart paths.

Lesson plans & materials	Ready-to-use but compressible	Provide materials that are **ready-to-use** yet **compressible**: basic (45–60') + extended (90–120') variants, in reorderable blocks.	Blocks: introduction–game–consolidation–check; each block states minimum target and "what is lost if cut".
Materials format	Real school usability	Ensure formats are genuinely usable in school settings (fast access, readable on tablet/mobile, scrollable).	Responsive layouts; print-friendly versions; one-click download; avoid "hard-to-navigate" PDFs.
Platform support	Modularity as a feature	Make basic/extended variants and modular blocks first-class objects supported by platform navigation and playlists.	Link variants; "short pathway" vs "full pathway"; add to playlist as a single unit (module + materials).
Mechanics vs content	Keep concepts central	Prevent play mechanics from overriding cybersecurity content: make the action–concept link explicit via micro-feedback and micro-tasks.	Prompts ("why is this safe?"), reminders/signals; rewards linked to safe choices, not only progression/collection.
Assessment (light)	Make learning visible	Provide lightweight, sustainable assessment tools that fit lesson time and age group and can be reused.	3–5 item pre/post micro-quizzes; observational checklists; printable/exportable; used as closure of the cycle.

Table 28: Quick checklist for designers and developers

DOs	DON'Ts
• Build for lesson continuity (non-invasive help + recovery) so classroom flow is protected. • Provide compressible, reusable materials and lightweight assessment that fit real time constraints.	• Don't rely on sharing "files only". Without context, resources are not reusable at scale. • Don't let progression/collection dominate. Keep the action–concept link explicit throughout.

6.4 Recommendations for researchers

The pilot and teacher interviews confirm a recurring pattern in cybersecurity education for children aged 8–13, namely that what appears "effective" in controlled settings may fail in real classrooms if it does not account for orchestration constraints (time, device availability, connectivity, classroom management) and for the mediation role of teachers. At the same time, the evidence suggests that engagement alone is not a proxy of effective learning. Educational value is amplified when play is integrated into structured pathways (before–during–after) and supported by lightweight assessment and consolidation activities. For researchers investigating and implementing experimental solutions, this implies that evaluation and design research should prioritise ecological validity, mixed-method triangulation, and replicable documentation of context and adaptations. Research should also take seriously the "transmedia" nature of game-based learning ecosystems: outcomes depend not only on the game but on surrounding resources (lesson plans, prompts, debriefing tools, guides) and on the socio-technical conditions enabling adoption and sustained use. Finally, as research often involves minors and collects behavioural traces, a privacy-by-design and data minimisation approach is essential to preserve trust and facilitate ethical scaling.

Table 29: Recommendations for researchers

Focus area	Recommendations	Implementation tips
Ecological validity	Design studies around realistic classroom constraints (time, devices, network instability, teacher workload).	Capture "classroom conditions at a glance" (duration, devices per pupil, connectivity, class size, teacher role, disruptions) and report them systematically.
Mixed-method triangulation	Combine learning indicators with teacher-mediated evidence (observations, debriefed artefacts, and short interviews) to avoid overreliance on observational reporting.	Use a minimal common core: (a) short pre/post items, (b) structured observation notes, (c) teacher reflection prompts after each session.
Outcome definition	Measure beyond engagement: focus on decision-making, transfer to daily situations, and vocabulary/concept clarity appropriate to age group.	Use scenario-based micro-tasks ("what would you do?") and child-friendly explanations; link each task to a target skill/competence.
Lightweight assessment	Adopt low-burden formative assessment aligned with classroom rhythms, avoiding long tests and complex analytics dashboards.	Prefer 3–5 item quizzes, exit tickets, short reflective prompts, or group debrief checklists; keep scoring transparent to teachers.
Context + adaptation tracking	Treat adaptations as data, not as noise: document what teachers change and why (timing, grouping, scaffolding, materials).	Provide an "adaptation log" template (what changed / reason / observed effects) and include it as study artefact.
Replicability & reporting	Publish reproducible protocols and artefacts (lesson scripts, prompts, rubrics, metadata), not only results.	Use a minimal metadata standard (age group, prerequisites, duration, resources used, known issues, adaptations) and share it with the dataset.
Co-design with practitioners	Involve teachers early as partners in research questions, measures, and feasibility checks.	Run short co-design cycles (45–60 min) to refine instruments; validate wording and burden with teachers before deployment.
Ethics, privacy, trust	Apply data minimisation and reversible consent; avoid collecting unnecessary personal or sensitive traces.	Clearly separate operational school data from research data; anonymise by default; provide opt-out pathways and transparent explanations to schools and families.
Equity & inclusion	Ensure materials and measures work across diverse schools and learners (language, SEN, different levels of digital familiarity).	Include accessibility checks, alternative formats, and differentiated pathways; report differential patterns and barriers explicitly.
Knowledge transfer	Translate findings into actionable guidance (for teachers, designers, policy-makers) rather than standalone academic outputs.	Produce short "practice notes" per study: what worked, for whom, under what conditions, and how to implement.

Table 30: Quick checklist for researchers

DOs	DON'Ts
• Build for lesson continuity (non-invasive help + recovery) so classroom flow is protected. • Provide compressible, reusable materials and lightweight assessments that fit real-time constraints. • Don't rely on sharing "files only". Without context, resources are not reusable at scale. • Don't let progression/collection dominate. Keep the action–concept link explicit throughout.	• Don't equate engagement with learning effectiveness without evidence of transfer or decision quality. • Don't impose heavy assessment or data collection that increases teacher burden or undermines trust. • Don't report outcomes without describing the implementation context and the socio-technical conditions. • Don't collect fine-grained traces by default: avoid non-essential data and ensure reversible consent and anonymisation.

6.5 Recommendations for policymakers and education authorities

The evidence gathered through teacher training, classroom piloting, and follow-up interviews in SuperCyberKids suggests that cybersecurity education for children aged 8–13 can be integrated effectively into formal schooling when policy choices address two interconnected dimensions: curricular legitimacy (where and how cybersecurity fits within learning objectives, progression, and assessment); and implementation capacity (teacher professional development, time allocation, infrastructure, and support). In practice, teachers tend to adopt cybersecurity resources when these are aligned with existing subjects and school priorities, come with ready-to-use materials, and remain feasible under everyday classroom constraints (limited time, devices, and connectivity).

For policymakers, this implies moving beyond one-off initiatives. Sustainable integration requires a clear framework, age-appropriate learning outcomes, structured teacher support, and procurement and governance models that preserve trust (privacy-by-design) while enabling scale and quality assurance.

Table 31: Recommendations for policymakers and education authorities

Policy area	Recommendations	Implementation tips
Curriculum integration	Embed cybersecurity education in the formal curriculum with **progressive learning outcomes** (8–13) and clear links to digital citizenship and transversal competencies.	Define a progression map (e.g., 8–9, 10–11, 12–13) and associate each level with expected behaviours/decisions, not only vocabulary.
Time allocation	Provide protected time through **micro-modules** that fit existing schedules (e.g., 30–60 minutes + short consolidation).	Recommend "minimum viable pathways" (e.g., 3 sessions) and "extended pathways" (6–8 sessions) for schools to choose from.
Teacher professional development	Institutionalise CPD on cybersecurity education, focusing on **pedagogical mediation and classroom orchestration**, not only technical content.	Offer blended CPD (short, synchronous + self-paced) and provide reusable lesson plans, scripts, and facilitation prompts.
School leadership enablement	Equip school heads and coordinators to support adoption (planning, resources, scheduling, data governance).	Provide leadership briefings and planning templates; integrate cybersecurity actions into school improvement plans.
Resource quality assurance	Establish quality criteria for educational resources (age appropriateness, inclusivity, usability, evidence, privacy).	Use a simple rubric for approval/endorsement; require metadata (age, duration, prerequisites, devices, accessibility features).
Infrastructure and access	Reduce inequalities by ensuring minimum infrastructure conditions and offline/low-tech alternatives.	Support shared device strategies, downloadable activities, and printable kits; include guidance for low-connectivity environments.
Assessment and recognition	Encourage **lightweight formative assessment** and recognise schools' efforts with certificates/badges aligned to learning outcomes.	Recommend exit tickets, scenario tasks, and class debrief checklists; define recognition mechanisms that do not require high-stakes tests.
Procurement and sustainability	Use procurement models that include training, updates, support, and maintenance—not only the tool itself.	Require vendor/provider obligations: onboarding, teacher guides, updates, accessibility compliance, and clear support channels.
Data governance and privacy	Adopt privacy-by-design and data minimisation as default, especially with minors; ensure transparency to families.	Provide standard DPIA[6] templates and guidance; separate operational school data from research/analytics data; require anonymisation by default.
Monitoring and scaling	Track adoption and impact through indicators that value feasibility and learning transfer, not just usage metrics.	Collect minimal indicators (reach, session completion, teacher feedback, observed learning behaviours, barriers) and use them to iterate policy and support.

[6] Data Protection Impact Assessment

Table 32: Quick checklist for policymakers and education authorities

DOs	DON'Ts
• Build for lesson continuity (non-invasive help + recovery) so classroom flow is protected. • Provide compressible, reusable materials and lightweight assessments that fit real-time constraints. • Don't rely on sharing "files only". Without context, resources are not reusable at scale. • Don't let progression/collection dominate. Keep the action–concept link explicit throughout.	• Don't equate engagement with learning effectiveness without evidence of transfer or decision quality. • Don't impose heavy assessment or data collection that increases teacher burden or undermines trust. • Don't report outcomes without describing the implementation context and the socio-technical conditions. • Don't collect fine-grained traces by default: avoid non-essential data and ensure reversible consent and anonymisation.

7 Pathways to implementation

According to the good practices that emerged from the SuperCyberKids piloting process and the resulting recommendations presented in Section 6, this section proposes an operational path for integrating cybersecurity education in primary and lower secondary schools (8–13 year old pupils). It exploits, adapts and modifies (where possible) the solutions developed within the SuperCyberKids project. Nevertheless, it should be emphasised that the recommendations in Section 6 are general in nature, regardless of the approach used in the SuperCyberKids project, and can be applied independently of it.

That said, the results of the SuperCyberKids piloting activities have demonstrated the effectiveness of the approach proposed by the project, which, while maintaining a firm focus on ensuring methodological rigour, has flexibility as its hallmark. The elements that characterise the SuperCyberKids ecosystem (i.e., learning framework, curriculum, lesson plans, gamification platform and analysis tools) can facilitate the practical application of these recommendations in educational actions, which can be implemented in the field and sustained over time.

The aim of this concluding section is to offer an end-to-end guide that makes it easier to (i) start activities in a sustainable way, (ii) consolidate their continuity over time, (iii) extend and scale them at the level of the institution or school network, and (iv) clarify their alignment with curricula and frameworks.

Specifically, SuperCyberKids supports the implementation of this path through an integrated ecosystem composed by:

- The SuperCyberKids Learning Framework clearly defines skills and expected outcomes.
- The curriculum organises progression into modules and micro-activities.
- The games and lesson plans translate objectives into ready-to-use learning experiences.
- The platform supports delivery, continuity and reuse.
- Finally, analysis tools enable light monitoring geared towards improvement and scalability.

In this section, these components are explicitly referred to in each phase of the roadmap to help schools and school networks move from experimentation to stable adoption.

7.1 An implementation roadmap: from the "minimum sustainable" to scaling

To ensure the effective adoption of the approach defined in the project, we propose a progressive approach, designed on a linear sequence of phases aimed at minimising organisational burden and risks while guaranteeing educational quality and replicability.

Table 33: SuperCyberKids implementation roadmap

Phase	Main SuperCyberKids Assets	Expected output
Phase 1 - Start-up	Lesson plans ready; games (digital/analogue); guided access to platform	1-2 micro-modules completed; debrief; minimal evidence
Phase 2 - Consolidation	Curriculum + Framework; platform for continuity/reuse; game catalogue; lesson plan repository	Stable modular path; differentiation; reuse of materials; structured feedback
Phase 3 - Scaling	Governance + platform; resource packages; analysis tools/KPIs; internal training	Integration into the school/network plan; monitoring; sustainability and replicability

7.1.1 Phase 1 – Start-up

The aim of the first phase (approximate timeframe: 2–6 weeks) is to introduce key concepts through short, highly guided activities, keeping the preparation workload and technical complexity low.

SuperCyberKids supports the start-up by providing streamlined and easily adaptable lesson plans that guide timing, resources and inclusive variations, as well as games that make core concepts (e.g., passwords, anti-phishing, and privacy) immediate and motivating. At this stage, the platform can be used in a guided and linear mode to reduce technical friction and maintain focus on the classroom experience, while evidence collection remains deliberately minimal (exit tickets and teacher checklists) so as not to increase the workload.

In practice, launch can be achieved with a minimum set of components:

- 1–2 micro-modules (one or two lessons each) on core concepts (e.g., passwords/access security, phishing/attention to signals, privacy and personal data);
- Ready-to-use materials (streamlined lesson plans), with estimated times, resources and variations for different levels;
- Guided debrief (10–15 minutes) to consolidate what I have learnt, where I can apply it, and common mistakes;
- Light assessment: 3–5 questions or a checklist (short pre/post or exit ticket).

Success criteria

The activity fits into the actual school timetable and can be repeated by a teacher without external support.

7.1.2 Phase 2 – Consolidation

In this phase (2-4 months), the objective is to stabilise teaching and organisational practices, ensure continuity between lessons, and gather minimal evidence useful for incremental improvement.

During consolidation, SuperCyberKids assets help to provide structure and continuity: the curriculum organises the sequence of modules and teaching progression (prerequisites, modularity, transversality), while the learning framework makes objectives and skills explicit and allows for verification that all areas are covered in a balanced manner. The platform facilitates the reuse and management of materials (courses, repositories, versions), and the analysis tools support a regular feedback cycle that allows activities to be corrected and improved without weighing down the design.

Standard implementation typically includes the following components:

- Modular plan: 4–6 distributed lessons (also transversally across multiple disciplines);
- Differentiation strategies: variations for heterogeneous classes and special educational needs;
- Orchestration routines: clear rules for group work, instrument rotation, and time management;
- Internal repository of materials (school or network): lesson plans, activity sheets, rubrics, FAQs.

Success criteria

There are reusable resources and a routine that reduces the preparation load in subsequent editions.

7.1.3 Phase 3 – Extension and scaling

In this phase (approximately one school year), the objective is long-term integration of cybersecurity education into the curriculum, extending adoption to more classes and school complexes, and activating governance and monitoring mechanisms for scaling.

On the matter of scaling, SuperCyberKids offers a set of levers that make institutional adoption more realistic. The curriculum and learning framework provide a common language for formal integration (vertical curriculum, civic education, school plans). The platform enables user and course management, sharing between classes and controlled updating of resources. The catalogue of games and lesson plans allows for the adoption of replicable packages at school or network level. At the same time, a platform dashboard of indicators and analysis tools supports informed decisions on governance, sustainability, and procurement.

Standard implementation typically includes the following components:

- Integration into the school plan (vertical curriculum, civic education, school educational plan);
- Structured training: communities of practice, mentoring between teachers, onboarding for new teachers;
- Light but continuous monitoring: adoption and quality indicators (see Section 7.4);
- Family involvement: micro-information kit and home-school "bridge" activities.

Success criteria

The activity is sustainable without depending on individual school "champions" and can be replicated in multiple schools/classes.

7.2 Roles and responsibilities

To make implementation sustainable, it is useful to clarify from the outset who does what: this distributes the workload more evenly and reduces dependence on key individuals. The following RACI matrix (R=Responsible, A=Accountable, C=Consulted, I=Informed) proposes a basic division of tasks, adaptable to the size of the school and the resources available.

Table 34: Roles and responsabilities matrix

Activities	*Teacher*	*Digital/ innovation coordinator*	*Headteacher*	*IT Support*	*Families*	*Researchers/ Designers*
Module selection and planning	R	C	A	I	I	C
Preparation of materials (lesson plans, resources)	R	C	I	I	I	C
Technical setup (accounts, devices, network)	C	C	I	R	I	C
Class management and orchestration	A/R	C	I	I	I	C
Debrief and light assessment	A/R	C	I	I	I	C
Feedback collection and improvement	R	C	I	I	C	A/R (if in trial phase)
Repository and reuse of materials	R	A/R	I	I	I	C
Policy, privacy and consent	C	C	A	R (for technical aspects)	C/A (for authorisations)	C

Practical note: in small schools, some roles may overlap; however, the matrix remains useful because it highlights responsibilities and interdependencies and helps prevent organisational overload.

7.3 SuperCyberKids Enactment Tool revised

In the project, the SuperCyberKids Enactment Tool kit (designed for piloting activities in the Deliverable D5.2 and updated here) corresponds to an integrated set of frameworks, curriculum, platforms, games, lesson plans, and analysis tools. The added value is the possibility of adopting ready-made resources and, at the same time, collecting light evidence to adapt and scale the intervention over time.

To prevent the guidelines from remaining abstract, an implementation kit is proposed that schools can adopt and adapt. The kit consists of essential artefacts and is designed to encourage reuse and co-design.

1. Basic kit (Start)
    a. Streamlined lesson plan (1–2 pages) with:
        i. objectives, prerequisites, actual times, materials, inclusive variations and adaptations;
        ii. typical pitfalls and solutions (e.g., timing, group management, technical difficulties).
    b. Debrief script (10–15 minutes) with guiding questions and examples of key messages.
    c. Exit ticket/mini-quiz (3–5 items) + quick reading criteria.
    d. Privacy and tool use sheet (for teachers and families, accessible language).
2. Standard kit (Consolidation)
    a. Lightweight skills rubric (observation of behaviours and awareness, not just correct answers).
    b. Adaptations sheet (inclusion, differentiation, SEN/SLD management).

   c. Teacher feedback template (what worked/what didn't work/timing/engagement/technical difficulties).
   d. Organised repository (naming convention, versioning, minimum metadata: age, duration, prerequisites, tools, licence).
3. Scaling kit (institute/network)
   a. Curriculum alignment map (see Section 7.5) + cross-disciplinary examples.
   b. Internal training plan (micro-modules for teachers + peer mentoring).
   c. Indicator dashboard (adoption/quality/organisational well-being – see Section 7.4).
   d. Guidelines for procurement and sustainability (costs, maintenance, minimum requirements, accessibility).

7.4 Minimum adoption and quality indicators

Scalability requires evidence but should not increase the management burden. We therefore propose a minimum set of indicators, collected using simple tools (checklists, short questionnaires, and essential logs where available).

In the SuperCyberKids context, evidence can be collected at two complementary levels: (i) "teacher-friendly" evidence (checklists, exit tickets, light rubrics) and (ii) platform-enabled evidence (e.g. module completion, session continuity, resource use), when available and in compliance with privacy and data minimisation.

A. Implementation indicators
   a. Coverage: number of classes/hours delivered/modules completed.
   b. Continuity: percentage of activities completed without interruptions or resets "from scratch".
   c. Reuse: materials reused (with minimal changes) vs. created from scratch.
   d. Technical stability: number of significant technical incidents per session.
B. Education quality indicators
   a. Observed engagement: participation, collaboration, persistence in tasks.
   b. Conceptual understanding: improvement on 3–5 key items or rubrics.
   c. Transfer: ability to apply rules/principles to new examples (including in debriefing).
   d. Inclusion: presence of adaptations implemented and perception of accessibility.
C. Organisational sustainability indicators
   a. Perceived teaching load: preparation and management time (short self-assessment).
   b. Internal support: availability of contact person/IT and response times.
   c. Curriculum alignment: explicit links to subjects/civic education/school plans.

Recommended use: collect this data on a quarterly basis or at the end of the cycle to inform incremental improvements and scaling decisions.

7.5 Curriculum and framework alignment: how to make it explicit

In the SuperCyberKids model, curriculum alignment can be seen as a value chain that makes integration easier and more traceable: the Framework defines what to develop in terms of cybersecurity skills; the curriculum organises how to distribute them over time in a progressive and modular way; the Resources (games and lesson plans) translate these objectives into concrete actions in the classroom; the Platform supports how to deliver and maintain continuity (pathways, reuse, resource and activity management); finally, the Evidence (light assessment and feedback collection tools) allows for iterative improvement of activities and supports consolidation and scaling decisions.

In general, schools integrate innovative pathways more easily if they can clearly see where to place the activities and what educational objectives are needed. For this reason, we propose a three-level approach, ranging from immediate curricular links to more formal mapping, which is useful when consolidating and scaling adoption at the school or school network level.

Level 1 – "Direct" curricular anchors

This level identifies the most natural curricular spaces in which to insert cybersecurity modules and activities, making it easy to integrate them into regular schoolwork.

- Civic education/digital citizenship: responsible online behaviour, rights and duties, respect and safety, and protecting oneself and others in digital environments.
- Technology/IT: account and credential security, data management, informed use of devices and networks, and basic concepts adapted to age.
- English/first language: critical analysis of digital messages and texts (phishing, manipulation, persuasive language, fake news), recognition of communicative signals and intentions.

Level 2 – Cross-curricular anchors

In addition to their place within specific subjects, many cybersecurity skills are developed by strengthening cross-curricular skills that cut across subjects and support learning in real-world contexts:

- Critical thinking and decision-making: assessing risks, recognising signals, and choosing age-appropriate prevention and protection strategies.
- Collaboration and communication: working in groups, negotiating rules, managing digital conflicts and netiquette, and assuming roles and responsibilities.
- Metacognition and self-regulation: reflecting on common mistakes, habits and automatic responses, understanding why certain online choices are risky, and how to correct them.

Level 3 – Formal mapping and curriculum integration guided by the skills framework

Unlike a simple list of topics or activities, the cybersecurity skills framework developed in SuperCyberKids is a real curriculum integration tool: it makes explicit what pupils need to develop (knowledge, skills, attitudes, and observable behaviours) and allows these outcomes to be linked both to direct anchors (where to place them in the curriculum) and to cross-curricular anchors (general skills that are mobilised and reinforced). In this sense, integration does not proceed "from the tools" (games or platforms), but from the skills, using the curriculum and teaching resources as means to achieve them in a progressive and verifiable way.

Operationally, a summary mapping is proposed, constructed in three steps:

1. Cybersecurity competence (SuperCyberKids Learning Framework): identification of the expected outcome and observable behaviours (e.g., recognising signs of risk, adopting preventive strategies, managing personal data, and assessing the reliability of messages and requests).
2. Curriculum anchors: linking the competency to a direct anchor (subject/area or civic education) and to one or more cross-curricular anchors (critical thinking, collaboration, metacognition, etc.).
3. Minimum resources and evidence: association with modules/activities (lesson plans, games, platform courses) and light evidence indicators (exit tickets, rubrics, observations), so as to support both teaching improvement and consolidation and scaling decisions.

This system also makes future interoperability with general frameworks easier. In particular, a significant next step will be the systematic mapping of the specific cybersecurity skills of the SuperCyberKids framework to the newly released DigComp 3.0 framework. This will facilitate adoption in contexts that

use DigComp as a reference, make results comparable, and support the institutionalisation of activities in the formal curriculum and in school plans.

7.6 Operational recommendations for policy and governance (implementation summary)

To enable formal integration and scaling, we suggest the following governance levers:

- Modular and progressive curriculum: provide recursive micro-modules (repeated annually) with increasing difficulty and transfer activities.
- Minimum adoption standards: define an essential set of outcomes (learning+behavior) and implementation indicators.
- Economic and technical sustainability: prefer solutions with minimum requirements, ease of maintenance and reuse of content; consider procurement that includes support and updates.
- Enhancement of the teaching community: recognising the role of "mentor teachers," facilitating sharing and reuse with repositories, and co-designing practices.
- Family involvement: promote home-school micro-actions to make safety messages and behaviours consistent.

In summary, the roadmap and tools proposed in this section transform beneficial practices and recommendations into an implementable path: start lightly, consolidate with routine and reuse, and scale with minimal governance and monitoring. This approach allows cybersecurity education to be integrated in a realistic, progressive manner that is aligned with the needs of schools, teachers, students, and families.

8 Conclusions

This handbook collects and systematises a set of evidence-based good practices for cybersecurity education in schools aimed at children aged between 8 and 13, and formulates operational recommendations for teachers, parents, designers/developers, researchers, and policymakers based on outcomes from the SuperCyberKids project.

The main contribution of this work is twofold. On one hand, it coherently integrates a theoretical and curricular framework with teaching resources and digital tools. On the other, it links these choices to evidence from teacher training, classroom experiments and interviews, clarifying the conditions that make the activities truly adoptable and sustainable.

The results show that the perceived effectiveness and quality of the learning experience depend less on the individual "artefact" (game or platform) and much more on the accompanying adoption infrastructure: lesson plans, support materials, scaffolding for classroom management, adaptability to school timetables, interdisciplinary integration, and simple monitoring and reflection mechanisms. From this perspective, the SuperCyberKids ecosystem defined in the project is configured as a value chain (framework → curriculum → resources → platform → evidence) that makes alignment with the curriculum explicit and facilitates both "light" implementation in ordinary contexts and more structured institutionalisation pathways.

The recommendations for stakeholders also outline a clear path for the co-design of high-quality resources and their iterative evolution: teachers as pedagogical orchestrators and mediators; parents as allies in home-school continuity; designers and developers as actors responsible for choices that combine engagement, content accuracy and security/ethics by design; and researchers as guarantors of robust assessment methods that are compatible with school constraints. For policymakers, the document offers

practical guidance to support the integration of cybersecurity education into the curriculum in a more informed way, enhancing disciplinary and cross-curricular anchors and promoting scalable adoption models.

Looking ahead, the work opens three priority directions: (i) strengthening formal mapping to reference frameworks and standards and consolidating "low-burden" assessment tools; (ii) supporting communities of practice and continuing education pathways, including school leadership figures; (iii) extending the model to new linguistic and cultural contexts while preserving quality, accessibility and data protection. Overall, this handbook is intended to serve as an operational reference for transforming cybersecurity from an episodic topic into stable educational skill development, integrated into school life and meaningful for the digital citizenship of young people.