Final management report
SuperCyberKids

Deliverable no. 1.1

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	**SuperCyberKids**
Document title	Final management report
Document Type	Deliverable
Document version	2, 30.1.2026
Previous version(s)	1,22.12.2025
Planned date of delivery	31 December 2025
Language	English
Dissemination level	Public
Number of pages	74
Partner responsible	CNR
Author(s)	Manuel Gentile (CNR); Salvatore Perna (CNR); Giuseppe Città (CNR); Paola Denaro (CNR)
With contributions by:	Anne-Sophie Van Vaerenbergh (ECSO); Luca Laszlo, (ESHA)
Revised by:	Jeffrey Earp (CNR) and Manuel Gentile (CNR)
Abstract	Deliverable D1.1 is the final management report of the SuperCyberKids project and provides a structured overview of progress, results and outcomes across the project lifecycle. It documents the completion of planned outputs and the development of a game-based educational ecosystem for cybersecurity education for children aged 8–13 (lesson plans, games and a gamification platform), together with evidence collected through large-scale piloting in multiple national contexts. The report summarises key lessons learned affecting adoption (e.g., variability in classroom use, usability and technical factors, the need for modular and flexible resources, and sustained support for teacher mediation) and outlines dissemination, exploitation and sustainability actions, including institutional collaborations enabled through a Memorandum of Understanding. Good practices and operational recommendations for teachers, parents, designers/developers, researchers and policymakers are consolidated in Deliverable D7.1.
Keywords	SuperCyberKids; Cybersecurity Education; Game-based learning
DOI	https://doi.org/10.17471/54038
How to cite	Gentile, M., Perna, S., Città, G., Denaro, P. (2025). Final management report. Deliverable 1.1 - SuperCyberKids project (ERASMUS-EDU-2022-PI-FORWARD - ERASMUS-LS - Project No. 101087250). DOI: https://doi.org/10.17471/54038

Table of Contents

List of Figures

List of Tables

1 Foreword and executive summary

The goal of this deliverable is to provide a summary of the achievements and objectives pursued in the project life cycle, displaying the overall project's progress and outcomes for each work package. This deliverable will form the basis for the final project report.

It summarises the implementation and results of the SuperCyberKids project, which developed and validated a game-based educational ecosystem for cybersecurity education for students between eight and thirteen years old. The report consolidates results and lessons learned for each work package and provides an informed basis for adoption, scalability, and sustainability actions beyond the project's duration.

Main results
The project fully achieved its implementation objectives: all 45 planned outputs were completed (11 deliverables and 34 internal reports), with minor delays managed transparently.
In terms of the operational availability of the ecosystem, the report highlights the integration between the platform, resources, and skills mapping (SEARCH/USE/UPLOAD), as well as the presence of a set of final deliverables covering games, the platform, the enactment toolkit, curriculum integration guidelines, and a handbook of good practices.

Evidence from pilots and early signs of uptake
The piloting activities (WP6) greatly exceeded the quantitative targets, involving 145 teachers (target 100), 480 pupils (target 200) and 87 managers (target 50), providing a solid empirical basis for assessing transferability and impact in different educational contexts.
At the same time, despite the platform having been active for a relatively limited period, encouraging initial signs are emerging: 149 registered users and 44 teachers responding to the questionnaire, for a total of 455 students involved.
The most used and appreciated resources are the interactive lesson plans that combine games and videos, which are perceived as easily integrable into teaching and consistent with learning objectives. In addition, 89% of teachers believe that the educational objectives have been achieved and express a strong intention to reuse the platform, indicating good prospects for sustainability.

Lessons learnt and remaining challenges
Adoption in schools required more effort than expected, highlighting the complexity typical of participatory initiatives; however, the targets were exceeded in the pilot countries. Some critical issues remain: inconsistent use of materials and technical problems related to gamification components. The report also points out the value of flexible and modular resources, differentiated by age/ability/national context, and the importance of ongoing support for teacher training.

Sustainability and scalability beyond the project
In terms of exploitation and policy impact, the consortium has launched a structured process (policy brief linked to the MoU and engagement initiatives), with significant results: the Memorandum of Understanding has been signed by 3 institutions, 20 schools, and 10 headteacher associations, representing 21,398 member schools (initiative still ongoing).
Dissemination has also been enhanced by positioning the final conference as a pre-event for the ESHA Biennial Conference 2025 in Rome, maximising access to European school leadership networks.

Key Takeaways
- Teacher mediation as a key enabler: materials work best when incorporated into guided activities and adapted to the classroom context.

- Gamification and interactivity increase engagement and understanding but require technical stability and guidance on use to avoid friction.
- Modularity and differentiation (age/ability/national contexts) are necessary conditions for adoption and scalability.

Policy relevance
The project offers practical tools that boost schools' and teachers' dedication and trust in cybersecurity education; while including it in school programs relies on larger institutional decisions, SCK helps to strengthen an ongoing trend by providing a ready-to-use system. The MoU and policy brief provide an operational channel for transferring results and recommendations to local/national/European levels, promoting uptake and collaboration beyond the project.

This final deliverable provides an overview of implementation, figures, results and sustainability. The translation of evidence into good practices and targeted recommendations for researchers, teachers, parents, designers/developers and policymakers (including guidelines for more informed and formalised curriculum integration) is consolidated in D7.1, which also contains details of the final evaluation.

2 Final management report

The goal of the SuperCyberKids project is to apply a game-based approach to enhance cybersecurity education for students between the ages of eight and thirteen. Games, in all their forms, including digital ones, have gained recognition as an effective method for implementing experiential learning pathways that foster skill acquisition. Of course, effective student education also requires suitable training of teaching staff, as well as the development of methodological and technological ecosystems to support teachers along all stages of an educational experience.

The first eighteen months of this three-year project, which began in January 2023, were dedicated to building the theoretical and practical foundations for the design and development of the SuperCyberKids ecosystem. The remaining eighteen months were dedicated to the piloting of the ecosystem in various Member States, together with its subsequent evaluation, refinement and rollout.

In the second part of the project, in addition to this deliverable, the ones listed in the following table were produced and published.

Table 1: Deliverables for the second part of the project

Deliverable Number	Name	Description	Due Date (in months)
D4.1	**Final version of the adapted and localized NABBOVALDO game**	D4.1 accompanies the release of the software related to the NABBOVALDO game, in its final adapted and localised version, complete with an API for integration into the gamification platform. The document sums up the translation and localisation work carried out and provides an overview of the main features of the game and how they can be integrated.	20
D4.2	**Final version of the adapted and localized SPOOFY game**	D4.2 accompanies the release of the software for the Spoofy game in its final adapted and localised version, complete with an API for integration into the gamified platform. The document summarises the translation and localisation work and presents the main features of the game, with reference to the technical integration requirements.	20
D4.3	**Guidelines targeting game designers**	D4.3 presents a methodology that, starting with a game (existing or developed ad hoc), guides the design of game-based educational activities suitable for specific school contexts. The methodology is	22

		aligned with the SuperCyberKids Learning Framework (D2.1) and includes the mapping of games to the framework's skills and the guidelines for competency-oriented design. The second phase introduces an operational tool (the Flexibility Table) for building contextualised, easily adoptable activities.	
D5.1	**Gamification platform and back- end tools**	D5.1 accompanies the release of the SuperCyberKids gamified platform (software). The document describes the implemented features, the user interface and the overall functioning of the platform, including a view of the APIs and middleware used for integration with external resources (e.g. games and content).	22
D5.2	**Enactment package for pilot uses cases**	D5.2 provides operational guidelines to support the use of the SuperCyberKids platform in schools during the piloting phase (WP6). The document is organised for three targets involved in the implementation (e.g., school/management, teachers, other actors) and collects the elements for three distinct enactment packages, designed to be used separately according to role.	22
D8.1	**Roadmap for the extension of the ecosystem on cybersecurity education**	D8.1 defines a roadmap to enable exchange, dialogue and mutual learning in a broad community of stakeholders interested in cybersecurity education. Based on the results of WP2–WP6, it identifies strategic objectives, engagement pathways and concrete actions for sustainability, scalability and transferability, with a focus on linking formal, non-formal and informal education and extending the ecosystem to additional school levels and digital competence domains.	33
D8.3	**Memorandum of Understanding**	D8.3 documents the objectives and development process of the Memorandum of Understanding (MoU), summarises its structure and content, and highlights its expected impact in terms of European policies and guidelines on education and digital literacy. It also defines the next steps for stakeholder engagement, including the initiative to collect signatures and endorsements within the framework of the final event (D8.2).	33
D6.1	**Guidelines targeting schools for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) - final version.**	D6.1 proposes a set of guidelines to support schools in integrating a game-based learning ecosystem on cybersecurity for pupils aged 8–13 into the curriculum, with particular reference to school administrators and teachers. The document outlines the rationale, enabling conditions and practical guidelines for adoption in the context of the European objective of strengthening digital awareness and resilience among young students.	35
D7.1	**Handbook of good practices on cybersecurity education in schools for children aged 8-13**	D7.1 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	36

		training, implementation and scalability of the SuperCyberKids ecosystem.	
D8.2	**Large-scale transnational event – Final conference**	D8.2 describes the context and positioning of the final project event within the ESHA Conference 2025 (Rome, 29–31 October 2025), highlighting the strategic consistency between the objectives of the SuperCyberKids event (28 October 2025) and the dissemination framework offered by the conference. The document explains the reasons for the timing and theme of the event and its contribution to the dissemination and consolidation of the project results.	36

All deliverables were published within the project deadlines, except for the last two, namely deliverable D7.1 and deliverable D1.1, which were submitted one month after the scheduled date[1].

The following table summarises all the achievements and results expected of the project throughout its lifetime. The table is a linguistically adjusted version of Table 1, which is reported in the Grant Agreement. Minor changes have been applied to aid/clarify review, while all the factual data (Obs, outputs, KPIs, scheduling) remained totally unaltered. All of the objectives were achieved.

Table 2: Objectives and Achievement Indicators

Ob.	**Sub-Ob.**	**Involved WP**	**Involved task**	**Achievement Indicators** (quantitative = target values)	**Outputs / Outcomes** R=Internal Report; D=Deliverable; MS=Milestone (Date of delivery)	**Status** (A=Achieved, P=Partially Achieved, N=Not yet started)
Ob.1	Ob.1.a	WP2	T2.1, T2.2	One published SuperCyberKids Learning Framework" (SUPERCYBERKIDS-LF)	D2.1 (M7)	A
	Ob.1.b	WP3	T3.1	One published EU reference framework for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren	D3.1 (M10)	A
	Ob.1.c	WP4	T4.1, T4.2, T4.3	Two digital games implemented	R4.1.1 (M20), D4.1 (M20), D4.2 (M20)	A

[1] The possibility of submitting after the project deadline was agreed upon by the project officer to allow the partnership to gather final feedback from the schools involved in the piloting process and to complete dissemination activities, in particular the collection of memoranda of understanding, which was particularly complex during a period that coincided with the Christmas holidays.

	Ob.1.d	WP5	T5.1, T5.2	One gamification platform implemented	R5.1.1. (M20), R5.1.2 (M22), D5.1 (M22)	A
Ob.2	Ob.2.a	WP6	T6.1	Pilot use cases: head teachers and teacher training initiatives delivered - At least all the fifty school heads involved in the pilot use cases participated in the training initiatives - At least all the one-hundred teachers involved in the pilot use cases participated in the training initiatives	R6.1.1 (M24), MS2 (M24)	A
	Ob.2.b	WP5	T5.3	One published enactment toolkit targeting head teachers, teachers, school children and their parents that helps them use the SCK game-based learning ecosystem on cybersecurity	D5.2 (M22)	A
	Ob.2.c	WP3	T3.3	Four published design documents for the enactment at different local levels (one for each pilot, draft to be validated through piloting)	R3.3.1 (M16)	A
		WP6	T6.2, T6.3, T6.4, T6.5	Four pilots implemented (Italy, Estonia and Germany, plus one EU-based pilot in English run in at least one Member State). At least 350 use cases produced (per country: 105 in Italy, 70 in Estonia, 70 in Germany, 105 EU-based; per target user: 50 school heads, 100 teachers, 200 schoolchildren)	R6.2.1 (M35), R6.3.1 (M35), R6.4.1 (M35), R6.5.1 (M35)	A
Ob.3	Ob.3.a	WP4	T4.4	One published set of guidelines targeting designers for the adaptation and localization (in other countries not covered by the	D4.3 (M22)	A

				Consortium) of other applied games		
	Ob.3.b	WP3	T3.2	One draft set of guidelines targeting head teachers and teachers on integrating the digital educational ecosystem into school curricula in different EU Member States (draft to be validated through piloting)	R3.2.1 (M12), MS1 (M12)	A
		WP6	T6.5	A finalised set of guidelines targeting head teachers and teachers on integrating the digital educational ecosystem into school curricula in different EU Member States, with guidelines and design document for the enactment at different local levels (final pilot-validated version)	D6.1 (M35)	A
	Ob.3.c	WP7	T7.2	One published Handbook of good practices on cybersecurity education in schools for children aged 8-13; handbook targets researchers, school communities, parents, designers in the education field, and policy makers.	D7.1 (M36)	A
	Ob.3.d	WP8	T8.1, T8.2	One Roadmap for the extension of the SUPERCYBERKIDS ecosystem to school levels outside the project's primary target and/or to other education providers and/or inclusion of non-native educational content in the domain of digital skills. - At least ten external partners express their interest in the Roadmap by signing a Declaration of Intent	D8.1 (M33)	A

		WP8	T8.1, T8.2	One large-scale transnational event to disseminate project results, foster exploitation, and help generate systemic impact - Final Conference - KPI: attendance by at least 50 individuals from various countries, of which at least 25 school heads (from at least 10 countries)	D8.2 (M36)	A
	Ob.3.e	WP8	T8.3	One signed Memorandum of Understanding, with Policy Brief. KPI - signed by at least: - three relevent educational institutions in three different Member States; - twenty-five school heads among those involved in the SUPERCYBERKIDS pilots; - fifteen school heads not involved in SUPERCYBERKIDS pilots	D8.3 (M33)	A

In the next sections, we provide a detailed description of the process that led to these achievements, as well as a summary of the project results.

2.1 WP1 - Project management and coordination (M1-M36)

The activities of the management WP were divided into three main tasks. Task T1.1 concerned the activities that the CNR, as Project Coordinator, carried out to ensure the efficient and timely achievement of the project's objectives.

The coordinator attended the European Commission's general kick-off event for Forward-Looking projects, which took place online between 14 and 16 February 2023. The CNR managed communications with the granting authority, both during the preparation phase and during project activities.

After the Grant Agreement was finalised in the preparatory phase, CNR negotiated the Consortium Agreement. The Consortium Agreement was defined to further detail the project organisation and management rules. The negotiation for the definition lasted 11 months. The relatively long duration of this agreement's defining process was due to the intensive verification of compliance with both the Grant Agreement and the internal regulations of the individual partner organisations.

To ensure on-time delivery and quality of project products, CNR defined a hierarchically distributed system of responsibilities involving, at different levels, the project coordinator and coordination partner's staff, the WP leaders, and the leaders of the related tasks.

In the framework of the project's kick-off meeting, held in Palermo on 2–3 February 2023, the partnership defined the members of all the planned project committees, namely the General Assembly

and the Steering Committee. Representatives from each WP leader formed the Steering Committee (SC), while one member from each partner formed the General Assembly. The General Assembly provided input into strategic and organisational issues, as well as defining the project standards and all project policies that must be formally and explicitly stated.

The CNR oversaw the project's overall management, setting up all of the methods and tools for efficient collaboration and communication within the Consortium.

From the outset of the project, it became evident that fostering communication among the partners was crucial, given the complexity and volume of tasks required, as well as the diverse backgrounds of the partners.

During the project kick-off meeting, the partners agreed to create a shared online space via the Microsoft Teams platform to facilitate communication and collaboration. This space allowed for improved email communication as well as the creation of a shared repository for collaboratively storing and working on project documents.

There were already clear internal and external deadlines set in the grant agreement's work plan. We further clarified these by creating and sharing documents in the workspace, which included a list of internal reports and deliverables, their due dates, and the individuals responsible for them.

Furthermore, in accordance with the quality plan defined within the framework of WP7, the partners responsible for the creation of the project products always worked using the sharing tools, enabling the other partners to continuously monitor and possibly revise the products.

The decision to hold a monthly appointment on the first Tuesday of each month served as another risk mitigation strategy. Before and after each monthly meeting, we prepared and shared a schedule and meeting minutes, respectively. These monthly meetings, also known as monthly update meetings, facilitated constant communication among the partners and facilitated resolution and decision-making.

During the second project meeting, held in Tallinn at the end of January 2024, the consortium agreed to introduce additional weekly online coordination meetings (in addition to the monthly update meetings) to facilitate the process of defining the European framework for the construction of curricula. Despite the time-consuming nature of these meetings, they enabled the partners to establish a shared understanding of the theoretical approach used to construct the framework. Moreover, during the same meeting the partnership agreed to share in the common workspace a living document including the key details of ongoing tasks and project deadlines.

The management of the project did not highlight any blocking issue. The only issue of any significance that we had to deal with concerned an official communication from CGI (one of the two Estonian partners) we received on 11 November 2024. The communication highlighted specific concerns regarding the possible use of the Nabbovaldo game for the Estonian trial during the preparation of the materials needed for the piloting activities. This communication highlighted critical issues regarding the data collected by the Nabbovaldo game in question and the type of scenarios described, which were not considered suitable for the target age group envisaged by the project.

To resolve this critical issue, a Steering Committee meeting was convened, which was held online on 27 November 2024. During the meeting, the Steering Committee decided to strengthen communication within the consortium, making it more direct and efficient, and to address issues in a timely manner by prioritising dialogue among partners and using the tools set up within the project. In particular, the consortium decided to continue organising weekly coordination meetings. In addition, the consortium reiterated the importance of keeping the shared to-do list (managed through a shared Excel file) regularly

updated and monitored to mitigate potential risks and ensure timely follow-up on agreed actions. Both measures were implemented and maintained to support more direct and efficient communication and to ensure timely issue resolution.

The main mitigation measure put in place to mitigate the risk raised by the CGI partner was the decision to finalise a feasibility study by mid-December, with the aim of estimating the time and effort required to re-engineer the Nabbovaldo game to ensure stronger alignment with the project's competency-based approach to educational activities. The feasibility study was finalised as planned and enabled the consortium to estimate both timelines and costs for the proposed reengineering. From a technical point of view, a new navigation mechanism was designed and implemented to allow teachers to run specific educational activities without needing to play through all game chapters sequentially. It was also recalled that the games were not a contractual project output; however, the partnership agreed to facilitate their update and coherent integration within the project ecosystem to maximise consistency with the learning framework and the related educational resources. Therefore, a budget transfer was implemented from the lead partner to GRIFO, as described and approved in the amendment submitted to the European Commission in July 2025.

CNR also took the lead in organising the subsequent meetings:

- The first virtual meeting, scheduled for June 2023 and held on 4 July 2023
- The second consortium meeting in Tallinn, held on 30 and 31 January 2024
- The second virtual meeting, scheduled for June 2024 and held on 25 June 2024
- The third consortium meeting in Brussels, held on 4 and 5 December 2024
- The third virtual meeting, scheduled for July 2025 and rescheduled to 6 October 2025
- The final consortium meeting and the final conference in Rome, held on 28 and 29 October 2025.

On the other hand, Task 1.2's activities focused on project monitoring and financial management. CNR, as coordinator, started active financial management of the project since receiving the letter of approval/funding from the EC. After signature of the Grant Agreement, pre-financing was distributed to each partner (40% of their grant allocation). Once the project commenced, CNR's SuperCyberKids financial manager configured a cloud storage space on OneDrive allowing each partner to upload their supporting documents. During the project kick-off meeting, the partnership was informed about the general principles of lump sum project financing, the cost categories within work packages, and supporting documents to be collected and stored if required, i.e. in case of an audit.

All partners fulfilled the financial record-keeping requirements specified for SuperCyberKids financial monitoring purposes. This included six-monthly uploading of timesheets and other supporting documents. The aim of this internal financial monitoring was to ensure:

- the person-months reported by each partner were in line with the budget and time schedule.
- completeness and cohesion of partners' supporting documents.

Moreover, as part of SCK's monthly online meetings, the coordinator (financial manager) kept partners fully updated on project admin and financial matters. This covered aspects like the level of work effort devoted to each WP, the ongoing status of required supporting documents, and the indications for clearly aligning budget spent with the actual work done by each partner. Partners have also received ongoing 'helpdesk' support for financial reporting, with bilateral meetings held with some partners for further clarification. During the project, the financial manager ran a number of internal admin/financial reporting sessions and produced a set of internal reports describing the progressive financial management and monitoring activities carried out every six months.

Task 1.3, led by CNR and carried out from the beginning of the project, has been implemented through a number of activities focused on identifying, assessing, and mitigating risks to ensure the project's smooth progress. In particular, Task 1.3 established a comprehensive Risk Management Plan (RMP), with the first version released in Month 3. This plan outlined procedures for risk identification, assessment, and management throughout the project's lifecycle. Additionally, a Risk Register was developed to document and monitor identified risks, assess their likelihood and impact, and plan appropriate responses. This living document was continuously updated based on ongoing risk assessments and discussions during Steering Committee meetings. Several coordination measures introduced under Task 1.1 (e.g., the shared workspace, regular meetings, and the shared to-do list) also supported risk mitigation and were tracked through the Risk Register.

The Steering Committee, composed of the Work Package Leaders, played a critical role in the risk management process. Their responsibilities included evaluating progress, proposing corrective actions, identifying remedial action plans, ensuring objectives and milestones were achieved, and monitoring activities. Each Steering Committee meeting included a dedicated discussion on risk management. A collaborative methodology using an online review form, titled "SUPERCYBERKIDS - Risk Register - Review Activity," was implemented to support the Steering Committee in updating the Risk Register by collecting comments, suggestions, and amendments from project partners.

The Advisory Quality Board provided external expertise to evaluate key project milestones, ensuring the quality of the educational content and curriculum. The Quality Manager, within WP7, coordinated closely with the Project Coordinator and the Steering Committee to monitor and manage quality-related risks, ensuring that all public outputs met the required standards.

Overall, the proactive and adaptive risk management strategy employed effectively addressed potential risks. Continuous updates to the Risk Register and regular discussions within the Steering Committee ensured early identification and prompt mitigation of risks, safeguarding the project's progress and success. The combination of well-defined roles, comprehensive planning, and a structured approach to risk management provided a solid foundation for navigating the complexities of the SuperCyberKids project.

The key critical risks and their management strategies during this period are detailed below.

- Internal project communication. Effective communication among project partners was paramount. To mitigate risks related to internal communication breakdowns, an online shared space was established to support asynchronous interactions through email and synchronous interactions via videoconferencing. Additionally, secure online file sharing was implemented to ensure data integrity and confidentiality. Continuous reminders and clear deadlines were set to facilitate timely and high-quality contributions from all partners.
- Delays in meeting internal deadlines and low-quality contributions. To address potential delays and ensure high-quality outputs, project partners were assigned tasks matching their competencies and interests. Internal deadlines were clearly identified and set with adequate notice. An internal review process under WP7 was established to monitor and guarantee the quality of project outcomes, including early submission of draft versions to ensure understanding of and adherence to expected standards.
- Organizational changes within the Consortium. To manage the risk of organizational changes, a Consortium Agreement was signed by all parties. This agreement outlined procedures for replacing any party if necessary, during the project's lifespan, ensuring continuity and stability within the consortium.
- Administrative and financial issues. These risks included the timely collection and verification of necessary formal administrative documents. The Project Coordinator took proactive measures to

collect these documents well in advance, ensuring they were checked and safely stored. The Consortium Agreement also included provisions for managing unexpected expenses, shared proportionally among all parties if deemed necessary and formally approved by the General Assembly.

2.2 WP2 - Definition of the SuperCyberKids Learning Framework (SUPERCYBERKIDS-LF) (M1-M7)

For the first seven months of the project, the partnership mainly focused on Work Package 2 (WP2) activities, together with preparative groundwork on dissemination and impact performed as part of WP8. WP2's goal was to create the *SuperCyberKids Learning Framework (SUPERCYBERKIDS-LF)* (**D2.1**), namely the conceptual foundation for the project's digital ecosystem of game-based cybersecurity education (**Ob.1.a**). The SUPERCYBERKIDS-LF was produced as a foundational support for the identification, definition, and formalisation of cybersecurity competences among the project's target student group (aged 8–13). It is intended to have both theoretical and applicative functions downstream in the project. As summarised in Fig. 1, the SUPERCYBERKIDS-LF is an evidence-based framework capturing and structuring competences for cybersecurity education for students aged 8–13.

The SUPERCYBERKIDS-LF's rigorously evidence-based development process entailed a thorough, multidimensional analysis of the field of cybersecurity for targets 8–13. Performed in Task 2.1, this analysis was based on three fundamental pillars:

- an in-depth literature review
- a survey of existing cybersecurity education initiatives, and
- a detailed analysis of digital competence frameworks.

Findings from these outputs provided a clear basis and solid scoping reference for the SUPERCYBERKIDS-LF, which was subsequently produced in Task 2.2.

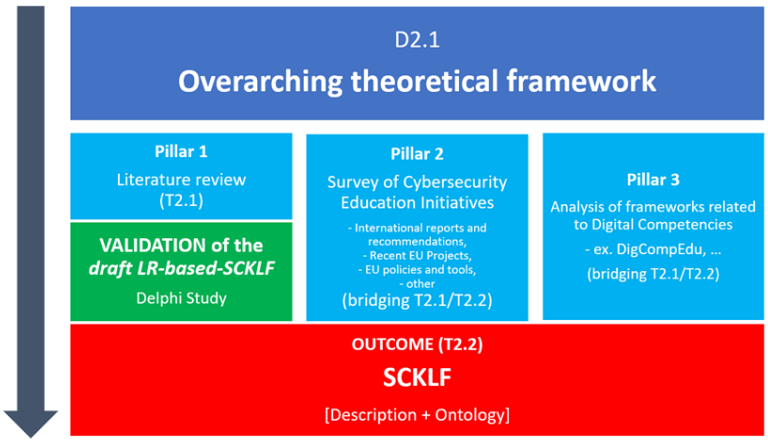

Figure 1: Overarching theoretical framework of SuperCyberKids

Pillar 1, the literature review, was carried out using a systematic approach of retrieval and analysis of academic articles available on the subject in major scientific databases, namely *ACM Digital Library*, *ACM Guide to Computing Literature*, *ERIC*, *IEEE Xplore*, *Web of Science*, and *PsycInfo*. Comprehensive research inquiry led to identification of 278 studies, 34 of which were identified as eligible for in-depth analysis in accordance with the quality criteria defined at the outset of the process. This analysis resulted in a classified skill mapping, i.e. a matrix of skills classified according to two dimensions: the US National Institute of Standards and Technology (NIST) Framework (https://www.nist.gov/cyberframework) and a high-level selection of recurring cybersecurity issues faced by 8–13-year-olds. While the identified

competences provided a comprehensive picture, a further in-depth study was required to verify their relevance and alignment with the reference target profile. This detailed validation step was performed through a Delphi study involving 18 experts from outside the partnership. The immediate result was enhancement and refinement of the skill matrix, with added value also being yielded for pursuit of WP8 goals, i.e. active engagement of a cohort of key international experts in the field from the very beginning of the project. The study about Pillar 1 were presented in a scientific paper published in the journal "Teaching and Learning in the Generative Artificial Intelligence Age"

> *Plintz, N., & Ifenthaler, D. (2026). From theory to practice: A content validation model for serious games in cybersecurity education. In Teaching and Learning in the Generative Artificial Intelligence Age (pp. 183-207). Cham: Springer Nature Switzerland.*

The second pillar, Pillar 2, the comprehensive survey of existing cybersecurity education initiatives, not only informed rigorous formulation of the SUPERCYBERKIDS-LF, but it also helped position the framework in the current European landscape of cybersecurity education for young learners and identify valuable sources of synergic contact and potential action downstream. The survey covered a multitude of initiatives active online both within and outside the European Union, with particular emphasis on those aimed at our demographic target. The analysis led to identification of 65 initiatives, which were subsequently codified and catalogued. We examined each initiative in terms of adopted training strategies, content type, and target. The results broadened our understanding of cybersecurity education beyond the theoretical level (gained from the Pillar 1 literature review), yielding practical insights into real-world implementations within a variety of contexts. The study and its findings were presented in a scientific paper published in the journal *Frontiers in Education*.

> *Manganello F, Earp J, Fante C, Bassi G, Fabbri S, Matteucci I, Vaccarelli A, Olesen N, de Vibraye A, Callaghan P and Gentile M (2024) Shaping the foundation of the SuperCyberKids Learning Framework: a comprehensive analysis of cybersecurity education initiatives. Front. Educ. 9:1375853. doi: 10.3389/feduc.2024.1375853*

So, the practical experience and results from the initiatives we studied have played a crucial role in defining the SUPERCYBERKIDS-LF, providing a base of real-world experiences on which to build an effective learning framework with appropriate scope, depth and structure.

Finally, the third pillar (Pillar 3) of the SUPERCYBERKIDS-LF was built from a comparative survey of nine important initiatives promoted in recent years by the European Commission (EC) on digital education and aim support for the development of digital skills. These initiatives include frameworks for digital skills/skills, self-assessment tools, and practical guides for innovation in learning and teaching processes, e.g. DigComp 2.2, SELFIE, SELFIEforTeachers. The investigation examined how these approached SCK-relevant issues like cybersecurity, online/social networking behaviour and safety, especially within the context of school-based digital education and literacy. It encompassed different levels, from educational policymaking through to classroom praxis, providing valuable scope and depth input for drafting the SUPERCYBERKIDS-LF, providing the framework with a stronger foundation and increased potential relevance for real educational contexts throughout Europe. As previously mentioned, support for the promotion of digital skills in education at various levels and contexts inextricably intertwines with the development of cybersecurity skills in (digital) education. Therefore, efforts on both fronts can be mutually beneficial in achieving the objectives of the European Commission's Digital Education Action Plan 2021-2027 (DEAP) (European Commission, 2020). The synergistic dialogue between the SUPERCYBERKIDS-LF and the abovementioned EC initiatives could prove extremely beneficial for the infosphere of digital education in Europe at conceptual, policymaking and operational levels. As mentioned, in its first 18 months SUPERCYBERKIDS has begun exploring paths to promote this dialogue and cross-fertilization and thereby boost dissemination, exploitation,

scalability, and sustainability of project results downstream (WP8). For instance, the SUPERCYBERKIDS-LF offers fresh perspectives on cybersecurity education issues, thereby enhancing the EC's ongoing efforts in the realm of digital skills in education, including potential enrichment/refinement of its frameworks, self-evaluation tools, and guidelines.

The next step was to identify, define, and formalise the competencies involved in the field of cybersecurity. In order to achieve this goal, we decided to leverage the formalism and applicative affordances offered by ontologies. Ontologies represent a valid and effective tool for formalising, manipulating and sharing knowledge in an unambiguous way. To this end, ontologies precisely define concepts within a given domain and express the various relationships that bind them. Initially, we explored the scientific literature to identify frameworks of validated and shared ontologies that had already addressed the formalization of the concept of competence. This analysis phase led to the selection of the ontological framework Comp2, defined by Paquette and colleagues. The SUPERCYBERKIDS-LF ontology has been defined based on the structure of concepts and reports offered by the Comp2 framework, which formally synthesises the project's framework of competencies. The ontology, published in the form of an RDF file, represents the initial heart of the knowledge base on which the subsequent phases of the project are based. To facilitate exploration of the ontology, a prototype online tool has been produced that allows step-by-step navigation of the elements and relations the ontology expresses. Currently for internal project use only, the tool is available at http://SUPERCYBERKIDS-LF.itd.cnr.it/explorer.

2.3 WP3 - Integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) (M5-M16)

In the fifth month of the project, WP3 activities officially started. WP3's overarching goal was to integrate and finalise the theoretical work performed during WP2 in preparation for operationalisation. WP3 represents a cornerstone for achieving the general project objective 1.b, i.e., the definition of a European framework for the integration of a game-based learning ecosystem for cybersecurity education in school curricula for students aged 8–13. WP3 activities involved three tasks: T3.1, T3.2 and T3.3.

From Months 5 to 10, the consortium pursued Task 3.1. This culminated in production of the second project deliverable, namely *D3.1 EU Reference Framework for the Integration of the Game-Based Learning Ecosystem on Cybersecurity into the Curriculum for Schoolchildren (aged 8–13) - Guidelines for Schools* (**Ob.1.b**). This was a preliminary version of the guidelines, which was updated and validated during the second half of the project with implementation of the pilot use cases, leading to publication of the final version (D6.1). D3.1 defines an EU framework integrating several educational dimensions, i.e., objectives, content, and evaluation metrics. D3.1 proposes a high-level structure for developing a cybersecurity education course organised into modules and educational objectives. Furthermore, D3.1 pays special attention to identifying effective methods for incorporating the game-based learning ecosystem into formal curricular activities.

Between Months 8 and 12, we performed activities under Task 3.2 - *Tools and guides for localization*. This involved defining methodologies and tools to facilitate the localization of the D3.1 framework in national curricula. The main goal of the task was to rearrange the SUPERCYBERKIDS EU framework into a generalised curriculum structure (first draft), in order to give policymakers, decision-makers, head teachers, and teachers a suitably education-oriented lens for producing appropriately curricula that fit their specific needs (**Ob.3.b**). The possibility of articulating the high-level curriculum structure into more operational localised curricula is a key element for successful integration of the overall SUPERCYBERKIDS ecosystem in specific contexts. Accordingly, Task 3.2 work specifically focused on seamlessly integrating the outcomes contained in deliverables D2.1 and D3.1, with an eye to eventual

operationalisation. A core aspect of this effort was correlating the expected learning outcomes from D3.1's educational objectives with the competence framework from D2.1. The structuring of the cybersecurity domain in learning modules was also revised, resulting in the definition of a competence-based framework organised in levels of complexity. The goal was to assist downstream stakeholders in producing more competence-based (rather than notional-centred) curricula, as they represent a prevailing trend and are better suited to the education of 8–13-year-olds. Fig. 2 provides a graphic representation of the resulting framework.

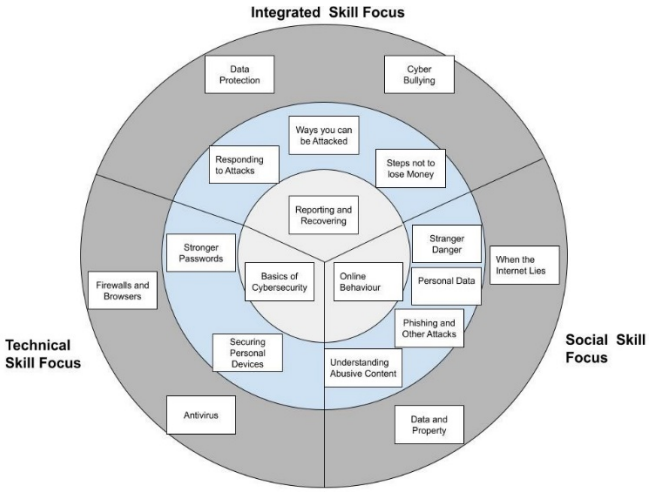

Figure 2: Graphic representation of SUPERCYBERKIDS reference framework

WP3 activities concluded with Task 3.3 (Localised Design for Pilot Cases), which engaged the partnership in design of localised pilot use cases (**Ob.2.c**). This undertaking lasted until Month 18 of the project. The purpose of the use cases is to enable application of the SUPERCYBERKIDS European framework's principles in specific national contexts through the planned pilot interventions. The results of this task have been described in Internal Report R3.3.1, which not only guides the implementation of the learning pathways that will be followed in the pilots but will also serve as an example of how the framework can be adapted to a variety of different contexts at the end of the project lifecycle (sustainability).

2.4 WP4 - Definition of game-based high-quality education content for cybersecurity education (M11-M22)

Activities in WP4 were carried out between Month 13 and 22 of the project. They largely involved the adaptation and localisation of the main pre-existing game-based learning content brought to the project by consortium partners: (i) the game "Nabbovaldo", provided by GRIFO and CNR (adapted in Task 4.2); and (ii) the game "Spoofy", provided by CGI (adapted in Task 4.3). This was the core learning content of reference for the general level curriculum defined in WP3 (**Ob.1.c**).

A key activity initiated in WP4 was the consortium analysis of the two partner-produced games through the lens of the competence framework produced in WP2. To develop an initial strategy for evaluating the content of the games, we conducted a systematic scoping review to identify a suitable approach. After an initial screening of four leading databases in the fields of psychology, education, and IT, we identified N=181 potential studies. The final strategy was then refined and developed based on N=18 studies. Once we had established this basis for comparison, we began to evaluate whether the competencies defined in the SUPERCYBERKIDS Learning Framework (WP2), as operationalised through the multidimensional analysis method (T2.1), could theoretically be acquired by playing the two games Nabbovaldo and Spoofy, in other words, whether the games provide a learning opportunity. Essentially, this step was about determining whether these games provided a theoretical framework for developing competencies. To do

so, input from 20 professionals in the fields of cybersecurity, cybersecurity education, and general education was collected. Experts were asked to play the games and assess whether, in their view, the game activities would help young learners acquire the skills indicated in the SUPERCYBERKIDS-LF. Overall, the results show that both games provide a solid theoretical learning opportunity for a wide range of cybersecurity competencies defined in the SUPERCYBERKIDS Learning Framework, particularly in areas related to online safety, data awareness, basic cyber threats, and responsible online behaviour. Experts identified several competencies as being well covered through gameplay, while others were assessed as only partially addressed, indicating the need for complementary educational materials or teacher mediation. The analysis also highlighted differences between the two games in terms of competence coverage, reflecting their distinct pedagogical focus and design choices. On this basis, the evaluation produced a set of targeted recommendations aimed at optimising and refining the games to strengthen alignment with the SUPERCYBERKIDS-LF and enhance their effectiveness for cybersecurity education.

The language-based content, cultural setting and references in the version of Nabbovaldo originally made available to SUPERCYBERKIDS were exclusively Italian. Task 4.2 involved the English localization of the game to be played in an English-speaking context. An English-language version was made available as early as Month 18 (two months before the scheduled deadline of month 20) to facilitate the mapping of competences being performed in Task 4.1. To facilitate the use of the serious game in the piloting phase, and specifically to cater to the social and context differences between the pilots, GRIFO also updated the game and provided a version in which specific chapters could be played individually. This update was made possible by an amendment that moved some of the budget from CNR to GRIFO.

Spoofy on the other hand was already multilingual but localisations in German and Italian were developed and implemented to meet project and pilots' requirements.

WP4 concluded with Task 4.4, in which know-how and outcomes from the other three WP Tasks were leveraged to develop methodological and technical guidelines for game designers and developers (**Ob.3.a**). The methodological part focused on promoting competence-based game design processes, while the second, more technical part promotes the integration of other (existing or custom-designed) games into the ecosystem the project is producing.

2.5 WP5 - Creation of toolkit and content to enact cybersecurity education in classrooms (M13-M22)

Work undertaken in WP5 centres on creating all the necessary elements for carrying out SUPERCYBERKIDS pilot activities. Task 5.1 specifically outlines the tools for monitoring and evaluating the learning paths that the pilots will implement. Consequently, we opted for the use of pre- and post-tests in the form of goal-based scenarios and constructed real-life situations, including school-related contexts, that are designed to reflect the everyday experiences of children as learning analyses to identify gaps in end-users' knowledge and measure learning progress. We classified these scenarios and situations according to the six domain areas of the SUPERCYBERKIDS-LF (abusive content, fraud, security, etc.) formulated in Task 2.1 and aligned them with the competence statements defined in the related ontology. Furthermore, to meet different evaluation requirements posed in different pilot settings, the consortium decided to implement two different tools: i) a separate online evaluation tool, hosted at the University of Mannheim, which does not store any data and only provides minimal feedback on the correctness or otherwise of 'hands-up', class-level test answers; ii) an evaluation tool integrated in the SuperCyberKids gamification platform. As described below, this is the subject of Task 5.2.

Work in Task 5.2 (Month 16 to 22) was aimed at creating the technological infrastructure to deliver cybersecurity education content to educational end-users. To this purpose, a specific instance of the gamification platform owned by the partner GRIFO was adapted to serve as middleware for the project's educational content ecosystem (**Ob.1.d**). Task 5.2 activities focused on creating a project-specific instance of the platform, called the SuperCyberKids platform, and embedding capabilities that allowed for the expansion of the standard functionalities currently on offer to include new ones. Essentially, this enhancement process was intended to render the platform more responsive, flexible and effective for use by teachers. A core action for achieving this was to create a direct connection between the platform contents (learning objects, game elements, lesson plans, etc.) and the competencies and skills specified in the SuperCyberKids Learning Framework created in WP2. During the months of Task 5.2 the efforts were focused on defining first by whom and then how the platform would have been used, including streamlining of activity flow when users browse the available learning resources. Three primary interaction modes were pinpointed, each with associated back-end platform functionalities that were implemented:

- **SEARCH**: locating suitable learning resources from those available on the platform, with the aid of competence mapping.
- **USE**: selecting in the platform's repository ready-to-use/repurpose lesson plans developed around 18 educational modules, which correspond to competences in six domains (Malicious Code, Safety, Abusive Content, Fraud, Data Protection, Preventive Techniques), and using them as basis for lessons or awareness-raising activities about cybersecurity in the classroom or at home.
- **UPLOAD**: adding new resources with appropriate tagging.

UIs for platform navigation have been created based on the initial desing in WP3, specifically R3.3.1.

Figure 3: UI for the navigation page of the SUPERCYBERKIDS platform

The design of the user experience (UX) and user interface (UI) was carried out to ensure the platform was both engaging and educational for the identified target audience. It was applied a specific scenario-based design, that takes into account the teachers' needs as main users of the platform. To this purpose, the work carried out by GRIFO relied on the specific expertise existing within the partnership, that includes experts in educational design, games and cybersecurity, plus, and above all, teachers (whose views are brought forward by ESHA), as representatives of target users. The platform and its accompanying technical report were completed by Month 22, as planned.

Finally, Task 5.3 was also dedicated to the creation of an implementation toolkit in three versions: for school leaders, teachers, and parents respectively (**Ob.2.b**). The first step was to create a Europe-wide set of SUPERCYBERKIDS open educational resources for young people's cybersecurity education. This effort began with mapping of each of the cybersecurity education initiatives identified in WP2 (see Deliverable D2.1) to the SUPERCYBERKIDSLF and related learning modules developed within Task 3.2. Furthermore, we added a short description of each initiative to guide end-users towards cybersecurity education initiatives of interest in Europe. The task concluded with the finalisation of lesson plans to be used in the pilots, contributing to the definition of the set of reusable and scalable tools needed to adapt the SUPERCYBERKIDS ecosystem to different national contexts and school levels. More details can be found in Deliverable D5.2.

2.6 WP6 - Implementation of pilot use cases in schools

Work Package 6 (WP6) was instrumental in operationalising the project's core objectives by translating the conceptual framework into real-world educational settings. WP6 coordinated the implementation of four distinct pilot use cases, in Italy, Estonia, Germany, and an EU-based context, each adapted to local educational systems and cultural contexts. These pilots were preceded by targeted online teacher training initiatives and followed by classroom experimentation using co-designed learning activities. The diversity of the pilot environments allowed the project to test the flexibility, relevance, and impact of the ecosystem across different educational landscapes.

The implementation of the pilot phase under WP6 was structured around four localised pilot use cases: Germany, Estonia, Italy, and an EU-based pilot conducted in English. Each pilot was adapted to its national or regional context and coordinated by a designated partner. The pilots were planned to run from January 2025 to November 2025, following a structured timeline that included teacher training (January 2025–November 2025) and final reporting (November 2025). ECSO provided strategic oversight and ensured consistency across pilots, while ESHA played a key role in mobilising school networks and engaging school leaders, particularly in the German and EU-based contexts. An important contribution was the additional development that GRIFO carried out on Nabbovaldo with the resources identified in the amendment. This allowed participants to use a version of Nabbovaldo in which individual chapters could be selected and played without the need to play the whole game, providing a version of the game that was usable with respect to the different cultural and social differences of the different pilot contexts.

Participation targets were defined across all pilots to ensure balanced engagement of teachers, schoolchildren, and school heads.

To achieve teacher participation, training sessions were organised within each pilot and delivered both online and in person. Following the training, teachers were invited to voluntarily trial an educational module. Participation targets were also established for schoolchildren to enable effective testing of the modules in classroom settings and to support meaningful evaluation of learning outcomes.

Targets for school head participation were reached via dedicated dissemination and engagement activities. These activities included:

- Participation in an international conference organised by ESHA in Rome, where school heads from diverse countries and educational contexts engaged in structured discussions related to cybersecurity education. A 'guided discussion rounds in groups' led by Luca Laszlo during the ESHA conference in the Mariot Park Hotel on the 28th of October. The event brought together 67 School Heads representing a diverse range of countries, including Canada, the USA, the Netherlands, Italy, Spain, Croatia, Slovenia, Bulgaria, Australia, Armenia, France, Norway, the UK, Iceland, Germany, Finland, Estonia, Denmark, Cyprus, Catalonia, Albania, Luxembourg, Lithuania, Kazakhstan, Ireland, Ukraine, Turkey, Switzerland, and Scotland. During the event, participants were invited to respond to a series of questions via Mentimeter, focusing on their role, professional background, and experience with cybersecurity education.
- Secondly a workshop in Istanbul by Peadar. He participated in a roundtable session with about 20 persons with Academics and schoolheads, presenting SUPERCYBERKIDS and talking a bout Cybersecurity for kids.

Table 3: Quantitative targets for WP6 activities

	Italy	**Estonia**	**Germany**	**EU-based**	**Tot per role**
School Heads	Target: 15 Reaching together with all pilots.	Target: 10 Reaching together with all pilots.	Target: 10 Reaching together with all pilots.	Target: 15 Reaching together with all pilots.	Target: 50 Reached: 87
Teachers (Teachers training)	Target: 30 Reached: 52	Target: 20 Reached: 43	Target: 20 Reached: 20	Target: 30 Reached: 30	Target: 100 Reached: 145
Schoolchildren	Target: 60 Reached: 315	Target: 40 Reached: 245	Target: 40 Reached: 40	Target: 60 Reached: 153	Target: 200 Reached: 480

Overall, WP6 activities far exceeded the initial quantitative targets. A total of 145 teachers (target: 100), 480 pupils (target: 200) and 87 school leaders (target: 50) were involved, providing a solid empirical basis for assessing the transferability and impact of the ecosystem in different educational contexts. Through the combination of training webinars, platform demonstration sessions and guided classroom trials, participation saw a high level of engagement from teachers and a positive response from students, particularly with regard to game-based activities. Below an overview of each pilot.

Italian Pilot

The Italian pilot, coordinated by CNR-IIT under the leadership of Giorgia Bassi, took place in Italy between 30/04/2025 and 31/10/2025 (first phase of teachers training) and 11/11/2025 and 18/11/2025 (second phase of teachers training). It followed a hybrid format, with teacher training conducted online and the piloting phase implemented directly in schools. Teachers were prepared through a series of three webinars, each lasting two hours, focusing respectively on the SUPERCYBERKIDS learning framework, the lesson plans, and the use of the platform. These sessions were supported by PowerPoint templates, and no adaptations were made to the original content or approach.

A total of 24 schools and 52 teachers participated in the training phase, while 10 schools and 14 teachers were involved in the piloting phase. The pilot reached 315 schoolchildren and generated a total of 165 use cases (Total use cases = #teachers in teacher training + #schoolchildren).

No parents or external stakeholders were involved. Teachers showed strong engagement throughout the activities, and schoolchildren responded with curiosity and enthusiasm. No significant challenges were reported, though future implementations may benefit from tailoring lesson plans to the specific needs and interests of each class group.

Informal feedback from teachers was positive, especially regarding the usability of the platform and the importance of cybersecurity education in schools. A more detailed analysis of pre- and post-questionnaires will be conducted under Work Package 7.

Estonian Pilot

The Estonian pilot, led by TLU and coordinated by Peadar Charles Callaghan, began on 26/03/2025 and the teachers finished on the 17/10/25 with a final interview on 11/11/25.

It was structured in two parts: an open webinar for all interested teachers, followed by a piloting phase in schools for those who chose to participate. Teacher preparation included a general webinar lasting 1.5 hours and a follow-up web meeting of approximately 45 minutes. The webinar used a shortened PowerPoint presentation based on partner materials. To better support teachers, a new localised lesson plan was created and added to the platform, with teachers encouraged to use whatever resources suited their classrooms.

So far, 41 schools have been represented in the webinars, and 7 schools have participated in the piloting phase. A total of 43 teachers attended the webinar, with 7 teachers involved in piloting. The pilot reached over 245 schoolchildren, and the total number of use cases is estimated at 288 or more, excluding school management participants. (Total use cases = #teachers in teacher training + #schoolchildren).

No parents or other stakeholders were involved. The decision to issue certificates to webinar participants proved to be an effective recruitment strategy. However, the pilot faced challenges due to delays and lack of clarity from the project side, prompting Estonian partners to take initiative and launch the pilot independently to meet deadlines. Teachers responded positively to the platform, although some technical issues were noted, and many expressed a desire for more content. Formal feedback will be analysed in detail under Work Package 7.

German Pilot

The German pilot, coordinated by UMA and led by Nicolai Plintz (Nicolai.plintz@uni-mannheim.de), was conducted between January 2025 and November 2025. It followed a hybrid format, with teacher training delivered online and the piloting phase carried out in schools. Teachers were prepared through a structured training process that included online sessions tailored to introduce the SUPERCYBERKIDS learning framework, lesson plans, and platform usage. A total of 12 school heads and 20 teachers participated in the training, with 2 teachers confirmed for the piloting phase. The pilot reached 40 schoolchildren, and the total number of use cases is 72, pending final updates. No parents or external stakeholders were involved in this phase. (Total use cases = #teachers in teacher training + #schoolchildren).

The training sessions utilised PowerPoint templates and other materials developed by the project partners. To better suit the local context, some adaptations were made to the content and approach, ensuring relevance and usability for German educators. One of the key successes of the pilot was the strong engagement from school leaders and the clear interest shown by participating teachers. However, challenges included limited time for implementation and difficulties in recruiting teachers for the piloting phase, which may have impacted the overall reach. For future implementations, it is recommended to provide more flexible scheduling options and clearer incentives for participation to ensure broader engagement.

Initial informal feedback from teachers highlighted the platform's ease of use and the value of introducing cybersecurity education in schools. While some technical issues were noted, the overall response was positive, with teachers expressing appreciation for the initiative.

EU Pilot

The EU-based pilot, coordinated by ECSO and led by Anne-Sophie Van Vaerenbergh (annesophie.vanvaerenbergh@ecs-org.eu), was conducted between January 2025 and November 2025. All teacher training sessions were delivered online, beginning with an initial outreach to identify European schools interested in participating. This led to two online training sessions on 26 February and 7 March, each lasting 1 hour and 30 minutes. A second round of outreach targeted additional English-speaking schools across Europe, resulting in two more sessions held on 3 and 4 September, also 1 hour and 30 minutes each. The training was supported by a customised PowerPoint presentation tailored to each audience and included live demonstrations of the platform to provide hands-on experience. The presentation was adapted to reflect the specific needs and backgrounds of the participating teachers.

In total, 30 teachers participating in the training sessions. 4 teachers completed the pilot. The pilot reached 153 schoolchildren, and the total number of use cases is 183. No parents or external stakeholders were involved in this phase. (Total use cases = #teachers in teacher training + #schoolchildren).

The structure and timing of the training sessions worked particularly well, with the 1 hour and 30-minute format and flexible scheduling helping to maximize participation. The main challenge was not recruitment, but maintaining teacher engagement, especially in collecting follow-up feedback on their experience and implementation.

While no specific improvements were recommended for future school-based rollouts, the feedback received has been valuable. Teachers expressed both satisfaction and constructive criticism. Some praised the training and platform, while others noted usability issues such as persistent help screens, difficulties scrolling PDF files, and challenges navigating the homepage. Suggestions included clearer guidance for interacting with the platform's interface, such as pop-up reminders to drag the map view. These insights will be further analysed under Work Package 7 to inform future development.

Besides the implementation of the pilot activities, a key outcome of WP6 is Deliverable D6.1, which brings together the final guidelines for integrating the game-based learning ecosystem on cybersecurity into school curricula. The document provides operational guidance for school administrators and teachers, illustrating the structure of the SuperCyberKids Learning Framework, the organisation of the 18 teaching modules, the use of lesson plans, the integration of educational games and how to use the platform. The guidelines are based directly on the evidence gathered during the pilot projects and offer concrete recommendations for adapting the ecosystem to different educational contexts, while maintaining consistency with the European reference frameworks on digital skills and cybersecurity education.

2.7 WP7 - Evaluation and Quality Assurance (M1-M36)

The activities carried out in the framework of WP7 allowed the consortium to constantly check the project's progress and prevent problems from arising. Great attention was paid to the monitoring of risks through the preparation of a risk register that was constantly updated according to the feedback from the various partners.

Furthermore, the advisory board's involvement made it possible to monitor the quality of the actions taken. Moreover, the external experts' feedback enabled us to enhance the quality of the deliverables.

Activities related to overall project quality assurance have been carried out all along the project. The mid-term quality and evaluation report and the final evaluation report have been issued. The consortium also submitted the main internal reports and deliverables to the Advisory Quality Board.

With regards to the mid-term quality report, it encompassed three key sections. Firstly, it detailed the state of advancement in the SUPERCYBERKIDS project, including progress in Work Packages (WPs), tasks undertaken, and outputs produced. Secondly, it outlined the quality revision process applied to deliverables and reports, highlighting the feedback received and how deliverables have been adjusted based on this feedback, ensuring alignment with project goals. Finally, it discussed the next steps, providing an updated roadmap for future project phases and ensuring smooth progress and improvement.

The design of the evaluation framework was prepared, discussed and refined together with project partners. The framework centres on four key evaluation questions and presents a Theory of Change of the SUPERCYBERKIDS project, a feature that has also been used as a reference to discuss and implement some of the project activities. In particular, the ToC has been used as a reference for the preparation of the materials and tools to be implemented in the pilot cases. An evaluation matrix has been developed as well as a part of the evaluation framework. This has made it possible to identify the most appropriate indicators to measure the effectiveness and quality of SUPERCYBERKIDS activities. Moreover, the evaluation framework represented a guideline for collecting information on the relevant evaluative dimensions, including the perceptions and opinions of the stakeholders involved in the project. Several tools for gathering quantitative and qualitative information have been developed. The mid-term evaluation report focused on two of the four evaluation questions set for the overall evaluation of the SUPERCYBERKIDS project. These questions dealt with the alignment of activities and outputs with the goals of the project, in terms of general quantity, (scientific) quality, and relevance for addressing the problems at stake.

Completing and updating the results of the mid-term evaluation, the final evaluation aimed to address all the questions included in the evaluation framework by drawing on the quantitative and qualitative information collected. This included information on the project's completion, data on participants in the project's initiatives, users of the SUPERCYBERKIDS platform, levels of resource utilisation, and opinions and perceptions gathered from participants in training activities and pilot projects through interviews, focus groups, and online surveys. Overall, the project fully achieved its implementation objectives: all 45 planned outputs (11 deliverables and 34 internal reports) were completed, with minor delays managed transparently. Involving schools and teachers required more effort than expected, highlighting the complexity of participatory initiatives, but the targets were greatly exceeded in all pilot countries. In terms of relevance, use and sustainability, the evaluation shows a strong consistency between the outputs and the project objectives. Although the SUPERCYBERKIDS platform has only been in use for a limited period of time, it shows encouraging signs: 149 registered users and 44 teachers responding to the questionnaire, involving a total of 455 students. The most used and appreciated materials were the interactive lesson plans with games and videos, which are considered easy to integrate into teaching and aligned with learning objectives. 89% of teachers believe that the educational objectives have been achieved and express a strong intention to reuse the materials in the future, indicating good prospects for sustainability beyond the end of the project. However, some critical issues remain, such as the uneven use of materials and technical problems related to gamification components. The report highlights important considerations. First, the central role of teacher mediation: materials are most effective when incorporated into guided activities and adapted to the classroom context. Second, gamification and interactive learning emerge as key mechanisms for increasing engagement and understanding of cybersecurity issues, especially in primary and lower secondary schools. At the same time, the project highlights the need for flexible, modular resources differentiated by age, skills and national contexts, as well as ongoing support for teacher training. Finally, in terms of relevance to education policy, the report notes a strengthening of the commitment to cybersecurity education at the school and teacher level. Although systemic integration into national curricula depends on broader

institutional choices, SUPERCYBERKIDS helps to consolidate an already existing trend by providing concrete tools and increasing the confidence of educators. The details of the final evaluation can be found in D7.1.

2.8 WP8 - Dissemination, Exploitation, Scaling-up and Sustainability of project results (M1-M36)

With respect to the objectives of communication, dissemination, exploitation, scaling-up and sustainability, the consortium, under the coordination of ESHA as WP8 lead, implemented continuous and structured activities to ensure visibility of the project, engagement of key target groups, and preparation for the long-term uptake of the SuperCyberKids results.

At the start of the project, the consortium developed a Dissemination, Communication and Engagement Plan, defining the overall strategy, phases, tools and target groups for dissemination activities, that was updated throughout the project. Dissemination actions were coordinated at consortium level and systematically monitored through a shared dissemination tracking table managed by ESHA, ensuring consistency, complementarity and compliance with Erasmus+ dissemination requirements throughout the reporting period.

The project website (https://www.supercyberkids.eu/) was developed by CNR and progressively updated by ESHA, serving as the central public access point for project information, news and publicly available results. Rather than creating new project-level social media accounts, the consortium agreed to leverage partners' existing communication channels, using the common hashtag #SuperCyberKids. This approach enabled partners to communicate in languages and formats appropriate to their established audiences, while ensuring coherent project visibility across local, national and European levels.

Through this strategy, the project benefited from ESHA's school leadership networks, ECSO's links to the European cybersecurity ecosystem, and partners' national and sector-specific outreach capacities. As part of the dissemination strategy, ESHA prepared four project newsletters at key moments of the project lifecycle. These were shared with partners in a flexible format to allow direct dissemination or integration into existing partner newsletters. Where relevant, newsletters were translated into national languages to support outreach at the local level. All newsletters were published on the project website and disseminated through partners' communication channels.

ESHA also supported partners in fulfilling mandatory dissemination obligations, including the correct use of the project's visual identity developed by CNR, acknowledgement of EU funding, and consistent tagging of communication outputs.

Dissemination and engagement activities were carried out by all partners in line with their roles and expertise. ESHA disseminated project information through its communication channels and informed its General Assembly members during four in-person meetings about the project's progress and relevance for school leadership and cybersecurity education, though 2 Biennial conferences attended by hundreds of school leaders and other in person events within its network, as well as through its magazine and newsletter. CNR disseminated the project through institutional websites, online media and social channels, including coverage on the Italian National Research Council website and specialised digital education outlets. CNR also organised a seminar at Didacta 2024 in Florence, supporting dissemination and pilot recruitment, and conducted public outreach through a science-focused radio programme. In parallel, CNR and the University of Mannheim contributed to scientific dissemination through peer-reviewed publications and presentations at international conferences, including AERA, CELDA and HELMETO. GRIFO focused its dissemination and exploitation activities on the development of the gamified platform and the adaptation of project games, presenting new features during a dedicated

webinar on gamification for training and promoting project-related developments through its professional channels. ECSO connected SuperCyberKids to the European cybersecurity ecosystem by promoting the project at European events and through its Road2Cyber platform, supporting long-term visibility within the cybersecurity skills and education landscape. CGI disseminated the project through national and international channels in Estonia, particularly in connection with the Spoofy game, while Tallinn University contributed through conference presentations and academic dissemination.

Exploitation activities were implemented in line with the project's Exploitation Plan (WP8), which identified exploitable results, target groups and channels and was updated throughout the project lifecycle. Exploitation channels included small-scale stakeholder events with school leaders, scientific publications, policy-oriented outputs, integration into existing educational and cybersecurity platforms, and the final conference. These activities supported early uptake, stakeholder feedback and alignment of project outputs with user and policy needs.

The project's final conference was organised as a pre-event to the ESHA Biennial Conference 2025 in Rome, maximising outreach to school leaders and education stakeholders from across Europe. The conference focused on sharing project results, experiences and lessons learned related to cybersecurity education in schools, with particular attention to curriculum integration, learning design, assessment and teacher professional development. An additional workshop was organised during the Biennial Conference to further extend outreach to participants unable to attend the final event.

In support of policy impact and long-term exploitation, the consortium developed a policy recommendation letter (policy brief) linked to the Memorandum of Understanding. The policy brief translates project results into concrete recommendations for stakeholders at local, national and European level, addressing identified policy gaps and proposing actions to strengthen cybersecurity education for children. In parallel, the consortium initiated to invite organisations to sign the Memorandum of Understanding, reinforcing commitment to continued collaboration and uptake beyond the project lifetime.

The following tables list the institutions, schools and associations of school leaders who have signed the Memorandum of Understanding to date. In total, three institutions, twenty schools, and ten associations of school leaders signed the Memorandum of Understanding, representing 21,398 associated schools.

These tables show that the results of this activity have far exceeded the objectives set out in the project. It should also be noted that this activity is still ongoing, and other schools and institutions (including two other Italian universities and the Sicilian regional education office) are in the process of signing the agreement, which has not yet been formalised solely due to the length of the formal approval processes required by these institutions.

Table 4: List of institutions that signed the Memorandum of Understanding

Country	Institution
Germany	Department of Information Systems - FOM University of Applied Sciences
Italy	Department of Engineering of the University of Palermo
Estonia	School of Digital Technologies

Table 5: List of schools that signed the Memorandum of Understanding

Country	Institution	Involved in the pilot
EU	"Ivan Vazov" Language School	no
Italy	Istituto Comprensivo 3 Modena	no
Italy	Istituto Comprensivo Statale "Rita Borsellino" Palermo	no
EU	International School of Budapest	yes
Italy	Istituto Comprensivo Li Muli	no
Italy	Istituto Comprensivo Statale Luigi Capuana	yes
Italy	Istituto Comprensivo Teglia	no
Italy	Istituto San Giuseppe	no
Italy	Istituto Comprensivo Beato Don Pino Puglisi di Villafrati	no
Italy	Istituto Comprensivo Don. Lorenzo Milani (ISA 1) - La Spezia	yes
EU	Metropolitan School Frankfurt gGmbH	yes
Italy	Scuola Secondaria Statale di Primo grado Viale delle Acacie	no
Italy	Istituto Comprensivo Daniela Settesoldi - Vecchiano (Pisa)	yes
Italy	Istituto Comprensivo Statale Giovanni Verga – Canicattì	no
Italy	Istituto Comprensivo Sampierdarena	no
Germany	Carl-Bosch-Gymnasium	yes
Germany	Esther-Bejarano-Gesamtschule	yes
Italy	Istituto Comprensivo Statale "Leonardo Sciascia" - Palermo	no
Italy	Istituto Comprensivo "Quasimodo" - Agrigento	no
Italy	Istituto Comprensivo Statale "Monti Iblei - V.E. Orlando" - Palermo	no

Table 6: List of school leaders associations that signed the Memorandum of Understanding

Country	Institution	Number of associated schools (for school leaders association)
Italy	Associazione Nazionale Dirigenti Scolastici - Sicilia (ANDIS)	NA
EU	ESHA board member for the Irish Primary Principals Network	3070
EU	Skolelederforbundet (Norway)	4000
EU	School Heads Association (Serbia)	300
EU	ESHA board member Scottish Boardmember SuperCyberKids	2700
EU	Associació de directius de l'educació de les terres de Lleida	58
EU	AXIA	65
EU	Association of School Principals Switzerland	2400
Italy	Associazione Nazionale Presidi - ANP	8525
EU	Revived Ukrainian Gymnasia Association of Principals (RGU)	280
Total number of schools associated with the networks involved		21398

Sustainability and scaling-up activities were embedded throughout the project and consolidated in the Scaling-up Strategy and Sustainability Plan. ESHA coordinated structured sustainability activities, including the use of an Education Scalability Checklist, sustainability workshops with consortium partners, and the development of local sustainability plans in Italy, Estonia and Germany. At European level, sustainability is supported through ESHA's school leadership networks and ECSO's Road2Cyber platform, providing a framework for continued dissemination, exploitation and scaling-up after the end of the project.

3 Final cost report

The financial management of the SUPERCYBERKIDS project has been carried out from the beginning of the project to assure that administrative and financial reporting obligations have been respected and in order to ensure that all partners used the resources within their budget according to the time schedule of each WP.

3.1 Financial Management Process

After the start of the project, in January 2023, the pre-financing has been distributed to each partner, and it has been transferred the 40% of the grant. A cloud storage service (Microsoft OneDrive) has been configured for the partnership to allow each partner to upload their own supporting documents. In the context of the kick-off meeting, held in Palermo in February 2023, the partnership was informed about the general principles for the eligibility of lump sum contributions, the cost categories of the WP,

and the supporting documents to be kept in case of a check or audit by the EC. After the kickoff meeting, CNR sent the link to the OneDrive financial folder to each partner, ensuring that each partner received the link only for their own folder. For good financial management by all partnerships, the Grant Agreement signed with the EC, the project Gantt, the description of activities assigned to every partner, and the associated budget have been sent to all partners. In addition to the main reference documents, the financial manager sent the partners the template to use for the timesheet.
In the first months of the project (March 2023) a risk management plan (RMP) has been developed by the coordinator. The main tool is the risk register that was updated during the lifetime of the project. Moreover, during the first year of the project, the Consortium Agreement was signed by all partners.
The purpose of the Consortium Agreement has been to specify with respect to the project the relationship among the partners, particularly concerning the organization of the work, the management of the project, and the rights and obligations concerning, inter alia, liability, access rights, and dispute resolution. The Consortium Agreement contains important articles relating to the payment arrangements, the monitoring, the reports, and general management of the project.
Another key step in the financial management process was the submission to the EC of the Periodic Report (end of August 2024). The report regards the activities carried out during the first 18 months of the project (from January 2023 until June 2024). At the beginning of October 2024, t~~T~~he letter of approval of the Periodic Report was received at the beginning of October 2024. Since the statement on the use of the previous prefinancing payment showed that more than 70% was used, we received an additional prefinancing payment of EUR 319,772.00. After that, ~~we~~ CNR transferred to all partners the second payment of the grant.

In order to structure a financial management process constantly updated and shared with project partners, during the lifetime of the project, the financial manager on behalf of CNR carried out 5 internal administrative and financial reporting sessions:

- the first session was held on 14 of July 2023;
- the second one within the consortium meeting held in presence in Tallin on 31 of January 2024;
- the third one on 16 of July 2024 to monitor the status of each partner/WP on an ongoing basis;
- the fourth was held on 4 of March 2025 to give to all partners feedback on the monitoring activity carried out on the status of the resources of each partner/WP from the beginning of the project until December 2024;
- the fifth session was held on 6 of October 2025 to give to all partners feedback on the monitoring activity carried out on the status of the resources of each partner/WP from the beginning of the project until June 2025

Moreover, every month, one online meeting was held with all partners to share the progress of the project activities. Within these online monthly meetings, the financial manager showed an update on the finances of each partner. Each partner was able to visualize the total number of working days and the number of months carried out for each WP. Moreover, guidelines, procedures and deadlines have been given to all partnerships to ensure that the budget spent will reflect the actual work done by each partner. The partners have been constantly supported via mail, Skype, Google meet, Teams, telephone for the financial reporting. Bilateral meetings were carried out by the financial manager with someone of the partners to clarify better some financial aspects of the project.

Face-to-face project meetings were an integral part of the management process. During the project lifetime, 4 face-to-face project meeting have been carried out:

- the kick-off in person meeting in Palermo in February 2023;
- the second meeting in Tallin in January 2024;

- the third meeting in Bruxelles in December 2024;
- the last meeting in Rome in October 2025.

Last but not least, a fundamental step in the financial management process coincided with the structuring of the amendments. In the first months of 2025, a first amendment has been prepared and submitted in the first days of July to the EC. The main changes requested concerned WP4, WP5 and WP6:

- WP4: cost of subcontracting (CNR) included in the original proposal has been transferred to personnel expenses since CNR utilised in-house personnel to translate the Nabbovaldo game.
- WP5: costs of subcontracting (CNR, UMA, TLU) included in the original proposal have been transferred to personnel expenses since the partners utilized in-house personnel to perform the translation for pilot uses cases.
- WP6: it has been needed reallocate part of the budget from CNR to Grifo to cover the additional effort required to update the Nabbovaldo game.

All changes requested in the amendment has been approved by the EC.

3.2 Financial Monitoring Process

Within the project, a periodic financial monitoring has been carried out on a semi-annual basis to ensure that administrative and financial reporting obligations have been respected and that all partners have used the resources within their budget according to the time schedule of each WP. Every six months, each partner was required to send their timesheets and other supporting documents to the coordinator (financial manager) or upload them to OneDrive shared folder for internal financial monitoring. Deadlines have been set for documents relating to each semester of each year:

- For the documents related to the first semester (January–June 2023), the first deadline was the first week of July 2023.
- For the documents related to the second semester (July–December 2023), the deadline was in the middle of January 2024.
- For the documents related to the first semester of 2024, the deadline was in the first week of July 2024.
- For the documents related to the second semester of 2024, the deadline was the 15 of January 2025.
- For the documents related to the first semester of 2025, the deadline was the 15 of July 2025.
- For the documents related to the second semester of 2025, the deadline was the 15 of December 2025.

The main aim of the internal financial monitoring was to check and monitor that:

- the person months reported by each partner are in line with their budget;
- partners have provided all the supporting documents, such as the timesheets of all people involved in the WPs;
- the costs used to calculate the lump sum match the actual costs of each partner.

All formal administrative documents needed have been collected by the financial manager quite in advance, checked and safely stored. Moreover, in order to collect all financial data, it has been required to all partners to send to the financial manager tables in which everyone filled in the working days worked in each WP and the corresponding person months.

3.3 Financial monitoring by work package

In this section we report an overview about the total working days and the person months and the total costs reported by each partner from the beginning of the project in January 2023 until December 2025 (36 months).

Table 7: WP1 - Summary of working days/PMs per partner from January 2023 to December 2025

PARTNERS	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
P1-CNR (ITD)	6	109	6,08	31.760,00 €	35.913,88 €
P1-CNR (IIT)	-	-	-		-
P2-GRIFO	5	95	5,75	10.182,00 €	11.364,08 €
P3-UMA	2	40	2	12.050,00 €	12.050,00 €
P4- ESHA	2	31,62	1,73	10.604,00 €	15.251,60 €
P5-ECSO	2	42,5	2	13.800,00 €	16.257,82 €
P6-AVANZI	2	55,3	2,95	12.270,00 €	12.294,52 €
P7-CGI	2	49	2,33	9.000,00 €	9.064,16 €
P8-TLU	2	49	2,3	7.000,00 €	12.833,84 €
TOT	**23 PMs**	**471,42 d.**	**25,14 PMs**	**106.666,00 €**	**125.029,90 €**

The table above reports the total number of working days and person-months carried out by each partner for WP1 from January 2023 to December 2025. As can be seen from the timesheets, all partners have reported all person months planned in the budget. Concerning the costs, for the partner Grifo the monthly cost has been overestimated during the budget planning. Consequently, Grifo increased the number of the person months to meet the total budget. Idem for the other WPs, in particular WP4 and WP5. For most other partner, instead, their actual costs are higher that the budget. As a result, for this WP, the actual costs are greater than the budget.

Table 8: WP2 - Summary of working days/PMs per partner from January to July 2023

PARTNERS	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED		BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
P1-CNR (ITD)	1	17,5	0,98	6,22 PMs	27.660,00 €	26.680,70 €

P1-CNR (IIT)	5	94	5,24			
P2-GRIFO	-	-	-		-	-
P3-UMA	5	100	5		25.000,00 €	25.000,00 €
P4- ESHA	-	-	-		-	-
P5-ECSO	2	51	2,36		11.000,00 €	16.286,00 €
P6-AVANZI	-	-	-		-	-
P7-CGI	-	-	-		-	-
P8-TLU	1	21	1		3.000,00 €	3.054,3 €
TOTAL	**14 PMs**	**283,5 d.**	**14,58 PMs**		**66.660,00 €**	**71.021,00 €**

The above table provides the total number of working days and person-months carried out by each partner for WP2 from January to July 2023 because this WP ended in July 2023. Each partner involved in this WP has reported all person months planned in the budget. For this WP, the actual costs are greater than the estimated costs.

Table 9 - WP3 - Summary of working days per partner form May 2023 to June 2024

PARTNERS	**BUDGET (PMs)**	**DAYS REPORTED**	**PMs REPORTED**		**BUDGET (TOTAL COSTS)**	**ACTUAL COSTS INCURRED**
P1-CNR (ITD)	2	36	2	3,06 PMs	14.132,00 €	16.647,23 €
P1-CNR (IIT)	1	19	1,06			
P2-GRIFO	1,71	20,50	1,71		4.268,00 €	4.264,00 €
P3-UMA	1	20	1		5.000,00 €	5.000,00 €
P4- ESHA	1	18,31	1		5.302,00 €	6.616,04 €
P5-ECSO	3	64	3		16.500,00 €	15.832,00 €
P6-AVANZI	1	16	0,84		4.320,00 €	2.707,45 €
P7-CGI	2	42	2		5.200,00 €	7.793,46 €

P8-TLU	14	256	12,1		42.000,00 €	25.175,11 €
TOTAL	**26,71 PMs**	**491,81 d.**	**24,71 PMs**		**96.722,00 €**	**84.035,29 €**

The table above outlines the total number of working days and the number of person-months each partner carried out for WP3 from May 2023 to June 2024. This WP started in May 2023 and finished in June 2024 instead of April.

Table 10: WP4 - Summary of working days per partner from January to October 2024

PARTNERS	**BUDGET (PMs)**	**DAYS REPORTED**	**PMs REPORTED**		**BUDGET (TOTAL COSTS)**	**ACTUAL COSTS INCURRED**
P1-CNR (ITD)	1	18	1	4,06 PMs	18.750,00 €	20.631,91 €
P1-CNR (IIT)	3	55	3,06			
P2-GRIFO	17,55	219	17,55		45.638,00 €	45.638,00 €
P3-UMA	6	120	6		30.000,00 €	30.000,00 €
P4- ESHA	-	-	-		-	-
P5-ECSO	-	-	-		-	-
P6-AVANZI	-	-	-		-	-
P7-CGI	8	168	8 PMs		20.800,00 €	31.632,31 €
P8-TLU	1	21	1 PM		3.000,00 €	5.398,98 €
TOTAL	**36,55 PMs**	**601 d.**	**36,61 PMs**		**118.188,00 €**	**133.301,20 €**

The table above reports the total number of working days and the number of person-months each partner carried out for WP4 from January to October 2024. As can be seen from the timesheets, each partner involved in this WP has reported all person months planned in the budget. The original proposal included subcontracting expenditures that were allocated for translating the Nabbovaldo game. CNR utilised in-house personnel to perform these activities during the implementation phase. The costs of subcontracting were consequently transferred to personnel expenses. For this WP, the actual costs are greater than the estimated costs.

Table 11: WP5 - Summary of working days per partner from January 2024 to February 2025

PARTNERS	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED		BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
P1-CNR (ITD)	3	55	3,06	5,18 PMs	23.778,00 €	30.132,56 €
P1-CNR (IIT)	2	38	2,12			
P2-GRIFO	24,03	230,5	24,03		51.542,00 €	51.542,50 €
P3-UMA	8	160	8		38.000,00 €	38.000,00 €
P4- ESHA	1	19,19	1,05		5.302,00 €	7.816,88 €
P5-ECSO	2	43	1,99		11.000,00 €	13.728,56 €
P6-AVANZI	-	-	-		-	-
P7-CGI	-	-	-		-	-
P8-TLU	3	83	4		11.000,00 €	11.100,85 €
TOTAL	**43,03 PMs**	**628,69 d.**	**44,25 PMs**		**140.622,00 €**	**152.321,35 €**

The table above presents the total number of working days and the number of person-months each partner carried out for WP5 from January 2024 to February 2025. The original deadline of the WP5 was in October, but during the last project meeting held in Bruxelles, it has been decided to postpone the end of this WP to February 2025. Moreover, since the partners utilized in-house personnel to perform the translation for pilot uses cases, the costs of subcontracting (CNR, UMA, TLU) included in the original proposal were consequently transferred to personnel expenses. Each partner involved in this WP has reported all person months planned in the budget; only TLU reported 1 person month more than planned. For this WP, the actual costs are greater than the estimated costs.

Table 12: WP6 - Summary of working days per partner from October 2024 to November 2025

PARTNERS	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED		BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
P1-CNR (ITD)	2	36	2	2,78	8.110,00 €	16.328,89 €
P1-CNR (IIT)	0	14	0,78			
P2-GRIFO	6,5	76,25	6,59		15.561,00 €	15.766,25 €

P3-UMA	2	43,6	2		10.900,00 €	10.900,00 €
P4- ESHA	4	6,31	0,34		21.208,00 €	3.364,94 €
P5-ECSO	5	104,5	5		27.500,00 €	32.383,96 €
P6-AVANZI	1	25	1,31		5.320,00 €	5.864,96 €
P7-CGI	2	42	2		7.200,00 €	7.951,59 €
P8-TLU	2	80	3,8		7.000,00 €	11.450,44 €
TOTAL	**24,5 PMs**	**427,66**	**23,82**		**102.799,00 €**	**104.011,03 €**

The table above reports the total number of working days and the number of person-months each partner carried out for WP6. After the evaluation and the approval of the amendment from the EC, CNR transferred part of the budget planned for this WP to Grifo. Consequently, the person months of CNR was reduced from 4 to 2 PMs. On the contrary, the person months of Grifo has been augmented to 6,5 PMs.

Table 13: WP7 - Summary of working days per partner from January 2023 to December 2025

PARTNERS	**BUDGET (PMs)**	**DAYS REPORTED**	**PMs REPORTED**		**BUDGET (TOTAL COSTS)**	**ACTUAL COSTS INCURRED**
P1-CNR (ITD)	3	54	3	8,25	26.042,00 €	37.908,4 €
P1-CNR (IIT)	3	94	5,25			
P2-GRIFO	1,75	21	1,75		4.368,00 €	4.368,00 €
P3-UMA	1	20	1		5.000,00 €	5.000,00 €
P4- ESHA	2	18,51	1,01		10.604,00 €	8.119,87 €
P5-ECSO	4	83	4		22.000,00 €	24.093,35 €
P6-AVANZI	8	179	8,22		34.560,00 €	34.580,35 €
P7-CGI	1	21	1		2.600,00 €	3.954,96 €
P8-TLU	1	24	1		3.000,00 €	3.342,03 €

TOTAL	**24,75 PMs**	**514,51**	**26,23**		**108.174,00 €**	**121.366,96 €**

The above table summarizes the total number of working days and the number of person-months each partner carried out for WP7 from January 2023 to December 2025. As can be seen from the timesheets, all partners have reported all person months planned in the budget: actually, CNR reported more 2,25 PMs more than planned; instead, ESHA reported 1 PM less than planned. For this WP, the actual costs are greater than the estimated costs.

Table 14: WP8 - Summary of working days per partner from January 2023 to December 2025

PARTNERS	**BUDGET (PMs)**	**DAYS REPORTED**	**PMs REPORTED**		**BUDGET (TOTAL COSTS)**	**ACTUAL COSTS INCURRED**
P1-CNR (ITD)	2	36	2	4,29	13.528,00 €	20.352,84 €
P1-CNR (IIT)	1	41	2,29			
P2-GRIFO	2	24	2		4.992,00 €	4.992,00 €
P3-UMA	1	20	1		5.000,00 €	5.000,00 €
P4- ESHA	6	192,32	10,5		31.812,00 €	71.375,34 €
P5-ECSO	5	105	4,91		28.400,00 €	24.689,08 €
P6-AVANZI	1	27	1,24		4.320,00 €	4.359,57 €
P7-CGI	1	21	1		2.600,00 €	3.501,96 €
P8-TLU	1	20	1		3.000,00 €	2.972,43 €
TOTAL	**20 PMs**	**486,32**	**25,94**		**93.652,00 €**	**137.243,22 €**

The table above shows the total number of working days and person-months carried out by each partner for WP8 from January 2023 to December 2025. As can be seen from the timesheets, all partners have reported all person months planned in the budget: actually, CNR reported more 1,29 PMs more than planned and ESHA reported 4,5 PMs more than planned. For this WP, the actual costs are greater than the estimated costs.

4 Final risk report

The SuperCyberKids project had a complex structure that could easily be subject to risks, which could affect the overall outcome of the project. More specifically, eight partners from five countries were involved, including the umbrella organisations operating at EU level in cybersecurity (ECSO) and school

leadership (ESHA), which, through their membership, brought together actors from across Europe. External stakeholders were continuously involved in the project activities through panel groups and small-scale enactment events, in addition to at least fifty school heads and at least one hundred teachers who directly participated in the pilot use cases.

Given the complexity of this project structure, both internal and external, problems and criticalities could arise. These could depend on the complexity of the objectives, on the profound differences among the contexts involved, on time constraints requiring strict adherence to planned deadlines, and on the distributed project structure.

With the aim of constantly keeping this aspect of the project under control, a specific task of WP1 (i.e., Task 1.3) was dedicated to identifying possible risks to the project, following *a risk management approach*.

4.1 The Risk Management Plan

Early in the project, a Risk Management Plan (RMP) was developed with the aim of identifying potential conflicts and risks that could arise over the project lifespan, assessing their potential magnitude, and defining a clear procedure for their identification, together with possible approaches and actions for their resolution, including tools supporting these procedures. The RMP defined procedures and responsibilities for conflict and risk management and represented the main reference over the three years of the project with respect to conflict and risk prevention, identification, and resolution, supporting the Project Coordinator and the project Steering Committee.

4.1.1 The Risk Register

The RMP defined a Risk Register (RR), which listed the main risks identified as potential drawbacks for the project, together with an estimate of their likelihood, their impact, and the actions envisaged to address or mitigate them. The RR, which was updated throughout the project, supported ongoing risk analysis and discussion and provided a concrete mechanism for sharing information about risks within the Consortium.

4.1.2 Conflict management in SuperCyberKids

The SuperCyberKids project conflict management was based on three main actions:

- Conflict prevention.
- Conflict identification.
- Conflict resolution.

4.1.2.1 Conflict prevention

To prevent potential conflicts among parties, a Consortium Agreement was prepared by the Project Coordinator and was signed by all parties. The Consortium Agreement was interpreted as a contract linked to the agreement with the funding body (i.e., the Grant Agreement) and aimed to integrate and specify obligations already included and regulated in the main contract.

Therefore, the main purpose of the Consortium Agreement was to specify relationships among the parties, in particular concerning responsibilities, work organisation, project management, and rights and obligations concerning liability, access rights, and dispute resolution. More specifically, the Consortium Agreement:

- Contained detailed information about the responsibilities of each party.
- Described the governance structure of the project.
- Undertook a precise approach to mitigating potential liabilities.
- Defined the general principles of financial provisions.

- Described foreground and access rights.

With specific reference to the governance structure of the project, it was defined fundamentally in terms of the characteristics and procedures of:

- **Project Coordinator.** This acted as the intermediary between the parties and the Granting Authority, as well as the supervisor of overall project progress. The coordinator, in addition to its responsibilities as a Party, performed the tasks assigned to it as described in the Grant Agreement and the Consortium Agreement. At the project coordinator level, there were a Scientific Coordinator (Manuel Gentile), a Project Manager (Flavio Manganello), and a Financial Manager (Paola Denaro). The Scientific Coordinator drove the Consortium to achieve target results from a scientific and research perspective. The Project Manager ensured that progress against milestones and deliverables and their quality were maintained. The Financial Manager managed and monitored project resources and schedules to ensure that financial reporting obligations were met and coordinated the collection of supporting documents from all partners.

- **Steering Committee.** This was responsible for work package coordination, planning, monitoring, and reporting. The Steering Committee was composed of the Work Package Leaders: Flavio Manganello (CNR, WP1 and WP2), Peadar Callaghan (TLU, WP3), Roberta Memeo (Grifo, WP4), Dirk Ifenthaler (UMA, WP5), Nina Olsen (ECSO, WP6), Davide Dal Maso (Avanzi, WP7), and Luca Laszlo (ESHA, WP8). They directed day-to-day technical planning and work within the Work Packages. The Steering Committee supported the Project Coordinator to ensure respect of milestones and achievement of project results by monitoring success indicators.

- **General Assembly.** This was the ultimate decision-making body of the Consortium. It was composed of one representative of each party duly authorised to deliberate, negotiate, and decide on all matters. The parties agreed to abide by decisions of the General Assembly. The members of the General Assembly were Ilaria Matteucci (CNR), Dirk Ifenthaler (UMA), Peadar Callaghan (TLU), Roberta Memeo (Grifo), Nina Olsen (ECSO), Petra van Haren (ESHA), and Catlyn Kirna (CGI).

- **Advisory Quality Board**. The project relied on external expertise through the sub-contracting of two Advisory Quality Board members (Iza Marfisi - Full Professor in Computer Science, LIUM, Université du Maine; Philip Geelkerken - Chair of the Supervisory Board of SIVON). In particular, one external expert was in the field of educational design (school curriculum design) and the other in the field of educational game design. Even though the Consortium included partners with expertise in these areas, independent external feedback on key project outcomes (e.g., milestone feedback and draft final evaluation feedback) was considered necessary. Sub-contracting was managed by AVANZI under WP7 activities. The Advisory Quality Board included two members, each financed with 5,000 Euros (travel included). Selection criteria were shared among partners and were approved in accordance with the Grant Agreement and the Consortium Agreement.

- **Quality Manager**. Within WP7, this role monitored and managed procedures related to the quality of any public output produced by the project. The Quality Manager, jointly with the Project Manager, regularly reviewed the PQP and its implementation based on a quality assessment checklist.

- **Internal Peer Reviewers' Board.** This is the body responsible for the quality of any public document (i.e., deliverable) produced by the project. It is composed of one person from each WP Leader's institution, the Project Coordinator and the Quality Manager.

4.1.2.2 Conflict identification

The project was structured so that the coordinator oversaw the detection of possible conflicts and sought to resolve them before they could affect the quality of project results.

Through its day-to-day activity, the Project Coordinator mediated between parties to mitigate potential risks of conflict. Risk management took into consideration possible conflicts that could arise within the Consortium and supported their identification. The Steering Committee was kept informed by the Project Coordinator about possible conflicts within the Consortium.

Conflict identification was carried out in coordination with WP7 (Evaluation and Quality Assurance). Each party was invited to inform the Project Coordinator about any possible conflict within the Consortium that could affect project quality. Conflicts could be formalised by one or more parties through a signed communication to the Project Coordinator.

4.1.2.3 Conflict resolution

Conflict resolution was handled through daily activities of support, mediation, and mitigation carried out by the Project Coordinator. When needed, the project decision mechanism followed the management structure in terms of roles, required activities, and responsibilities of the Steering Committee, the Project Coordinator, and the General Assembly. In addition:

- WP Leaders were required to inform the Project Coordinator of any significant unforeseen event (e.g., delays in deliverables or milestones) concerning their WP. The Project Coordinator, supported by the Steering Committee, then decided appropriate actions.
- Administrative monitoring and reporting of the project budget were the responsibility of the Project Coordinator and were reported to the Commission.
- The Project Coordinator and the Steering Committee acknowledged reports from the Quality Manager and the Advisory Quality Board and planned appropriate actions as needed.
- The Project Coordinator managed and monitored the project budget, oversaw the running of the project (including revising strategic objectives), and handled conflict resolution.

Final approval of major interventions, which could include:

- redistribution of resources within the Consortium,
- negotiation of modified targets, and/or
- proposed changes to the work plan,

was the responsibility of the General Assembly as the final decision-making body of the project.

Voting represented the method used to resolve conflicts and to implement changes in the Consortium structure. The Project Coordinator acted as the highest authority within the project. Internal decisions within each work package were taken by majority of WP participants. If no majority resulted, a vote proportional to participants' shares in that work package was applied. The same procedure was applied to internal task decisions.

In the event of a conflict, a conflict resolution procedure could be activated if one or more parties sent a formal and signed communication to the Project Coordinator. In such cases, the conflict was managed by the Project Coordinator and a group of three referees. Two referees were nominated by the parties in conflict and the third was nominated by the two referees already chosen. If the two referees failed to reach an agreement, the Project Coordinator nominated the third referee.

4.1.3 Risk Management

An important element of project management was the analysis, identification, and management of risks. Early risk identification and the definition of contingency plans helped speed up required reactions and mitigate negative consequences.

Risk management in the SuperCyberKids project included risk identification, risk analysis, response planning, and risk monitoring and control. The objective was to decrease the probability and impact of adverse events that could significantly affect project outcomes.

Figure 4 depicted, in general terms, the overall risk management process followed in the SuperCyberKids project. Each of the functions shown in the figure was discussed in the following sections.

Figure 4: Risk management process

4.1.4 Risk Management Planning

Risk Management Planning was the process of deciding how to approach, plan, and execute risk management activities in the SuperCyberKids project. Its main output was the Risk Management Plan, which stated the main elements and rules for risk management in the project.

The definition of the SuperCyberKids Risk Management Plan was based on the main project objectives, the expected results, and the main risks identified at proposal stage.

The Risk Management Plan defined the following elements:

- Risk categories.
- Risk probability and impact.
- Roles and responsibilities in risk management.
- Plan of activities.

4.1.4.1 Risk Categories

Risk categories provided a structure to ensure a comprehensive process for systematically identifying risks at a consistent level of detail. Risk categories were revisited during the project, and additional risks that did not correspond to the initial categories were identified when needed.

The risk categories for the SuperCyberKids project included:

- Risks related to project management.
- Risks related to internal project elements.
- Risks related to pilots and their organisation.
- Risks related to the external environment.

4.1.4.2 Definition of Risk Probability and Impact

The risk analysis process required that levels of likelihood/probability and impact were defined. For the SuperCyberKids project, both probability and impact were categorised into five levels: Very Low, Low, Medium, High, Very High.

The assignment of impact levels to identified risks was performed in accordance with the number of project objectives whose achievement would have been negatively affected by the occurrence of the risk. Project main outputs/outcomes were identified in the proposal according to three categories: Internal Reports, Deliverables, and Milestones:

- Internal Reports were documents related to specific tasks that presented information intended for circulation only within the project. They were not designed to be shared with EACEA and did not undergo the internal review process.
- Deliverables were linked to one or more tasks and represented outputs of that work. The number of deliverables was intentionally minimised (well below 15 as recommended), while other important outputs were formalised as internal reports. Deliverables were designed to be shared with EACEA and underwent an internal review process as defined by the Internal Peer Reviewers' Board.
- Milestones were important mid-term steps or results of the project.

Time was also considered: a risk affecting a high number of results but causing only a limited delay was considered less disruptive than a risk influencing only one result but causing a substantial delay.

Table 12 associates the impact risk level with the influence of the risk on results and schedule.

Table 15: Risk Impact definition

Impact	**Very Low**	**Low**	**Moderate**	**High**	**Very High**
On Project Objectives	One output affected	Two outputs affected	Three outputs affected	Four outputs affected	Five or more outputs affected
On Schedule	Minor delay *Less than 15 days*	Small delay *More than 15 days, less than 1 month*	Medium delay *More than 1 month, less than 2 months*	High delay *More than 2 months, less than 3 months*	Major delay *More than 3 months*

Figure 5 shows the combination of the different levels on the two axes of probability and impact generates a risk impact matrix, with five different levels: Very Low, Low, Medium, High, Very High.

Impact on Project Objectives	Impact on Schedule: Very Low	Low	Medium	High	Very High
Very High	Medium	High	High	Very High	Very High
High	Low	Medium	High	Very High	Very High
Medium	Low	Medium	Medium	High	Very High
Low	Low	Low	Medium	High	Very High
Very Low	Very Low	Low	Low	Medium	High

Figure 5: Risk Impact Matrix

Finally, as shown in Figure 6, probability and impact combinations generated a **risk severity matrix** with four levels: Sustainable, Moderate, Severe, and Critical.

Probability	Impact: Very Low	Low	Medium	High	Very High
Very High	Moderate	Severe	Severe	Critical	Critical
High	Sustainable	Moderate	Severe	Critical	Critical
Medium	Sustainable	Moderate	Moderate	Severe	Critical
Low	Sustainable	Sustainable	Moderate	Severe	Critical
Very Low	Sustainable	Sustainable	Sustainable	Moderate	Severe

Figure 6: Severity Risk Matrix

4.1.4.3 Roles and Responsibilities

As already mentioned, the Project Coordinator was responsible for coordinating and monitoring all risk management activities. This was carried out in coordination with the Steering Committee, the Advisory Quality Board, and the WP7 leadership (i.e., the Quality Manager).

In particular, the Steering Committee oversaw:

- evaluating WP progress and proposing corrective actions when needed;
- identifying remedial action plans in the event of deviations;
- ensuring that WP objectives and milestones were achieved;
- monitoring parties' activities, tracking and reporting effort, deliverables, and progress;
- integrating input from the Advisory Quality Board (WP7) and supporting parties in meeting requirements.

The Project Coordinator, with the support of the Steering Committee, worked to ensure adherence to milestones and achievement of project results by monitoring success indicators identified in the proposal.

The Advisory Quality Board evaluated key milestones to ensure quality from a user perspective. The WP7 Leader ensured the flow of information between the Advisory Quality Board and the General Assembly through the Project Coordinator. When needed, feedback was analysed by the Project Coordinator within the Steering Committee to identify remedial actions.

A continuous monitoring process was carried out focusing on success indicators, milestones, and achievement of results. Emerging problems were addressed as they were identified, and small remedial actions were implemented as soon as possible, enabling improvements and adjustments when needed.

Figure 7 shows the relations between WP1 (Management, Project Coordinator), WP7 (Quality Assurance, Quality Manager) and the other bodies for the management of Quality Assurance, Evaluation and Monitoring within the project.

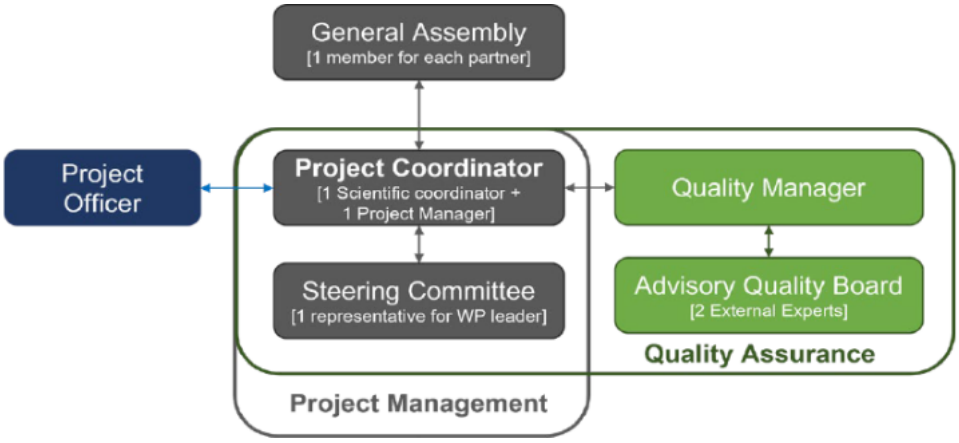

Figure 7: Relations between WP1 (Management), WP6 (Evaluation) and WP8 (Quality Assurance)

4.1.5 Development of the Risk Register

Risk item identification was based on a structured and consistent approach to ensure that all areas were addressed. The Risk Register included identified risks together with analysis and potential responses, enabling:

- quantitative assessment and ranking of risks;
- definition of alternative paths to reduce or minimise risk;
- monitoring and management throughout the project lifecycle.

4.1.5.1 Risk identification

Risk identification was the first step in the risk assessment process. It was performed by:

- reviewing documentation, gathering information, and analysing the validity of assumptions on which the project was originally conceived;
- discussing problems and issues with WP Leaders;
- gathering feedback from parties during meetings and by email;
- receiving feedback from EC officers.

The defined risk categories provided a structure to identify and classify risks systematically.

4.1.5.2 Risk Analysis

Risk analysis consisted of evaluating identified risks to determine likelihood/probability and impact and to establish a risk rating. The probability and impact definitions were used throughout the project.

Risks with high probability and/or high impact were treated as major risks requiring particular attention.

All team members were required to inform the Project Coordinator about any event implying a change in the risk assessment.

4.1.5.3 Risk Response Planning

The approach to handling significant risks was developed after risks were identified and assessed. Four options for risk handling were considered:

- *Avoidance* – applying measures to avoid the risk.
- *Mitigation* – performing tasks that reduced probability and/or impact to an acceptable level.
- *Transfer – transferring the risk to another party responsible for its management.*
- *Acceptance* – monitoring and controlling the risk to keep likelihood and impact at low levels when the risk was acceptable or no suitable strategy was identified.

For identified risks, handling techniques were evaluated in terms of feasibility, expected effectiveness, cost, schedule implications, and effects on technical quality and performance.

The Project Coordinator, in collaboration with the Steering Committee and relevant Task Leaders, developed and evaluated risk-handling strategies suited to project circumstances. Selected strategies were approved by the Steering Committee before implementation.

When approving a strategy, the Steering Committee also defined evaluation criteria to assess whether it was successful in minimising risk impact at that time.

The Project Coordinator monitored and controlled the performance of risk-handling actions in cooperation with the WP7 Leader. Partners directly involved in a risk were included in evaluating results against the previously defined criteria.

4.1.6 Risk Monitoring and Control

The Risk Management Plan was revised by all parties, which actively contributed to defining and evaluating reported risks. Project progress was continuously monitored for new and changing risks. Risk monitoring and control included:

- risk reassessment (identification of new risks and reassessment of existing ones);
- evaluation of the quality of project results, developed in cooperation with the WP7 Leader for project evaluation and quality assurance.

Risk monitoring and control were documented through recommended corrective and preventive actions which, once approved by the Project Coordinator in cooperation with the Steering Committee, were integrated into updated versions of the Risk Register.

4.2 Risk Register Data

The following table shows the trend in the risk register following updates to the perception of risks by project partners. In particular, the table highlights a change that occurred halfway through the project (coinciding with the interim report). Specifically, the table shows that the only risk considered critical had been downgraded to severe risk. Two other risks had been downgraded from severe to moderate. Conversely, other risks had seen an increase in their risk level. This process highlights the attention with which the partnership monitored the progress of the project.

Table 16: Risk Register Table

					Initial			**Interim**		
ID	**Date raised**	**Risk category**	**Risk description**	**WP(s) affected**	**Probability of the risk occurring**	**Impact if the risk occurs**	**Severity** *Likelihood * Impact.*	**Probability of the risk occurring**	**Impact if the risk occurs**	**Severity Likelihood* Impact.**

1	31/03/23	Risks related to the management of the project	Internal project communication	1	**Very Low**	**High**	**Moderate**	**Low**	**High**	**Severe**
2	31/03/23	Risks related to the management of the project	Delays in internal deadlines or low-quality contributions	All	**Very Low**	**High**	**Moderate**	**Low**	**High**	**Severe**
3	31/03/23	Risks related to the management of the project	Organizational changes in the Consortium	1	**Medium**	**High**	**Severe**	**Low**	**Medium**	**Moderate**
4	31/03/23	Risks related to the management of the project	Administrative/financial issues	1	**High**	**High**	**Critical**	**Low**	**High**	**Severe**
5	31/03/23	Risks related to internal elements of the project	Lack of dissemination and impact benchmarks	7;8	**Low**	**Low**	**Sustainable**	**Low**	**Medium**	**Moderate**
6	31/03/23	Risks related to internal elements of the project	Low usability of the toolkit and content implemented in the project	4;5;6	**Medium**	**Medium**	**Moderate**	**Low**	**Medium**	**Moderate**
7	31/03/23	Risks related to internal elements of the project	Availability of the project's website and sustainability the project results after the end of the project	8	**High**	**Low**	**Moderate**	**Medium**	**Medium**	**Moderate**
8	31/03/23	Risks related to pilot uses cases and their enactment	Inadequacy of the EU reference framework for localization	3,6	**High**	**Medium**	**Severe**	**Medium**	**Medium**	**Moderate**

9	31/03/23	Risks related to pilot uses cases and their enactment	Low participation of school heads and teachers to the online training initiative	6	**Low**	**High**	**Severe**	**Medium**	**High**	**Severe**
10	31/03/23	Risks related to pilot uses cases and their enactment	Few schools than planned attending project pilot use cases	6	**Low**	**High**	**Severe**	**Medium**	**High**	**Severe**
11	31/03/23	Risks related to pilot uses cases and their enactment	Issues in collecting feedback from the pilot use cases	7	**Medium**	**High**	**Severe**	**Medium**	**High**	**Severe**
12	31/03/23	Risks related to external elements	Impossibility to localize the EU framework in some countries	3	**Low**	**Low**	**Sustainable**	**Low**	**High**	**Severe**
13	31/03/23	Risks related to external elements	Low involvement of relevant stakeholders during the project	2;3;4;5;6;8	**Low**	**Low**	**Sustainable**	**Medium**	**High**	**Severe**
14	31/03/23	Risks related to external elements	Issues in the organization of the final conference	8	**Medium**	**Medium**	**Moderate**	**Low**	**High**	**Severe**
15	31/03/23	Risks related to external elements	Difficulties related to the long-term sustainability	8	**High**	**High**	**Critical**	**Medium**	**High**	**Severe**

In essence, as already indicated in the first part of this report, the management of the project did not highlight any blocking issue. The only issue of any significance that we had to deal with concerned an

official communication from CGI (one of the two Estonian partners) we received on 11 November 2024. The description of how this event was handled by the partnership is described on page 13 of this report.

4.3 Data Processing Risks

The partnership adopted a privacy-by-design and privacy-by-default approach, fully aligned with Regulation (EU) 2016/679 (GDPR), ensuring that the protection of personal data was not treated as a compliance add-on but as a structural dimension of project design, implementation, and evaluation. This approach was operationalised through three mutually reinforcing instruments:

- a Joint Controller Agreement (JCA) regulating shared controllership among partners;
- a specific Data Processing Agreements for ESHA, a partner acting as a processor;
- a comprehensive Data Protection Impact Assessment (DPIA) addressing risks related to data processing activities across all project phases.

4.3.1 Data governance model and allocation of responsibilities

Given the collaborative nature of the project and the fact that several partners jointly determined the purposes and means of personal data processing, the consortium formally adopted a joint controllership model pursuant to Article 26 GDPR. All of the partners, with the exception of ESHA, acted as Joint Controllers. The JCA clearly defined:

- the scope of joint control;
- the categories of data subjects and types of personal data processed;
- the purposes and means of processing;
- the allocation of responsibilities among Joint Controllers;
- mechanisms for cooperation, mutual assistance, and accountability.

The JCA ensured full compliance with Articles 24 and 26 GDPR and established a unified governance structure while preserving each partner's accountability within their institutional and national legal frameworks

4.3.2 Role of processors

Within the project, one partner processed personal data on behalf of the Joint Controllers, without determining purposes or essential means of processing. In particular, the European School Heads Association (ESHA) acted as a Data Processor for specific, limited processing activities related to stakeholder engagement and dissemination.

A dedicated Data Processing Agreement was put in place between the Joint Controllers and ESHA, in accordance with Article 28 GDPR, defining:

- the subject matter and duration of processing;
- the nature and purpose of processing;
- the categories of personal data and data subjects;
- the processor's obligations regarding confidentiality, security, and assistance to controllers.

4.3.3 Mapping of data processing activities

Children were involved in educational activities exclusively under the mediation of teachers and schools, and no directly identifiable data of minors were collected or stored. The primary data subjects were therefore the teachers, the school leaders, and the project stakeholders and experts. In line with the principle of data minimisation, only strictly necessary personal data was processed. These included:

- identification and contact data (e.g. username, email address);
- professional information (role, country, school affiliation);
- platform usage data (access logs, pages visited, content used);
- feedback and evaluation data, mostly collected in aggregated or anonymised form.

No special categories of personal data (Article 9 GDPR) were processed. No systematic profiling or automated decision-making was implemented. A detailed mapping of all data categories, tools, recipients and purposes was documented in the DPIA and annexed to the Joint Controller Agreement and can be consulted in Annex 2.

4.3.4 Legal bases and principles of processing

All data processing activities were grounded in clear and lawful legal bases under Article 6 GDPR, primarily through informed consent of participants for evaluation and research-related activities. The consortium ensured compliance with all GDPR principles, and transparency obligations were fulfilled through detailed information notices, informed consent forms, platform privacy policies, clear communication of data subjects' rights.

4.3.5 Data Protection Impact Assessment (DPIA)

Given the scale of the project, the cross-border nature of processing, and the involvement of an online platform, CNR carried out a Data Protection Impact Assessment in line with Article 35 GDPR. The DPIA aimed to systematically identify risks to the rights and freedoms of data subjects, assess their likelihood and severity, and define appropriate mitigation measures. The assessment covered the entire data lifecycle, from collection to deletion, across all pilot countries and technical infrastructures and was approved by CNR's Data Protection Officer (DPO). The DPIA identified potential risks including:

- unauthorised access to platform data;
- accidental data disclosure;
- re-identification risks in evaluation datasets;
- inconsistencies in data handling across partners;
- data breaches affecting trust and reputational integrity.

Importantly, the DPIA confirmed the absence of high-risk processing involving vulnerable categories, as no children's personal data were processed directly. For each identified risk, the consortium defined and implemented mitigation measures, including role-based access control and authentication mechanisms, secure hosting and encrypted data transmission, separation between identifiable data and evaluation datasets, anonymisation and aggregation of survey data, staff training and confidentiality obligations, and documented incident and breach management procedures. Based on these measures, residual risks were assessed as low and acceptable.

4.3.6 Technical and organisational security measures

Technical safeguards included secure cloud infrastructures managed by institutional providers, firewalls and access logging, encrypted connections (HTTPS), regular system updates and maintenance, and restricted administrator privileges. Moreover, the SuperCyberKids platform, managed by GRIFO, complied with best practices for web-based applications and published a dedicated privacy policy detailing security measures.

4.3.7 Data subject rights and transparency mechanisms

In line with Articles 12–22 GDPR, the Joint Controller Agreement established clear procedures to enable data subjects to exercise their rights, including:

- access;

- rectification;
- erasure;
- restriction;
- objection;

4.3.8 Data retention, archiving and deletion

Personal data will be retained only for the duration strictly necessary to fulfil project purposes and reporting obligations. As defined in the DPIA, identifiable data will be deleted within five years after project completion while anonymised and aggregated data may be retained longer for scientific research purposes.

5 Annexes

5.1 Annex 1: Financial monitoring by partner

P1: CONSIGLIO NAZIONALE DELLE RICERCHE

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	2	37	2	9.292,00 €	12.329,58 €
Researcher	2	28	1,56	10.500,00 €	8.430,37 €
Administrative	2	44	2,45	11.968,00 €	15.153,92 €
TOTAL	**6**	**109**	**6**	**31.760,00 €**	**35.913,87 €**

WP2: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO JULY 2023

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	17,5	0,98	4.646,00 €	5.363,94 €
Researcher	3	12	0,67	15.750,00 €	6.078,64 €
Technician	2	82	4,57	7.264,00 €	15.238,11 €
TOTAL	**6**	**111,5**	**6,22**	**27.660,00 €**	**26.680,70 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	2	47	2,62	10.500,00 €	15.160,58 €

Technician	1	8	0,44	3.632,00 €	1.486,55 €
TOTAL	**3**	**55**	**3,06**	**14.132,00 €**	**16.647,23 €**

WP4: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO OCTOBER 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	3	39	2,17	15.750,00 €	13.632,36 €
Technician	1	34	1,89	3.000,00 €	6.999,54 €
TOTAL	**4**	**73**	**4,06**	**18.750,00 €**	**20.631,90 €**

WP5: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2024 TO FEBRUARY 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1,4	25	1,39	7.146,00 €	8.376,82 €
Researcher	2,73	49	2,73	13.000,00 €	17.695,02 €
Technician	1	19	1,06	3.632,00 €	4.060,72 €
TOTAL	**5**	**93**	**5,18**	**23.778,00 €**	**30.132,56 €**

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	18	1	4.646,00 €	6.505,87 €
Researcher	1	32	1,78	5.250,00 €	9.823,02 €

TOTAL	**2**	**50**	**2,78**	**8.110,00 €**	**16.328,89 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	18	1	4.646,00 €	6.066,46 €
Researcher	2	51	2,85	10.500,00 €	14.473,87 €
Technician	3	79	4,40	10.896,00 €	17.368,07 €
TOTAL	**6**	**148**	**8,25**	**26.042,00 €**	**37.908,4 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	18	1	4.646,00 €	6.066,46 €
Researcher	1	21	1,17	5.250,00 €	5.786,46 €
Technician	1	38	2,12	3.632,00 €	8.499,91 €
TOTAL	**3**	**77**	**4,29**	**13.528,00 €**	**20.352,83 €**

P2: GRIFO

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	2,5	30	2,5	6.240,00 €	6.240,00 €
Administrative	2,5	65	3,25	3.942,00 €	5.124,08 €

TOTAL	**5**	**95**	**5,75**	**10.182,00 €**	**11.364,08 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1,71	20,50	1,71	4.268,00 €	4.264,00 €
TOTAL	**1,71**	**20,50**	**1,71**	4.268,00 €	4.264,00 €

WP4: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO OCTOBER 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1,75	21	1,75	4.368,00 €	4.368,00 €
Technician	15,80	198	15,80	41.270,00 €	41.270,00 €
TOTAL	**17,55**	**219**	**17,55**	**45.638,00 €**	**45.638,00 €**

WP5: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2024 TO FEBRUARY 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	12,75	81	12,75	20.160,00 €	20.160,00 €
Technician	11,29	149,5	11,29	31.382,00 €	31.382,50 €
TOTAL	**24,04**	**230,5**	**24,04**	**51.542,00 €**	**51.542,00 €**

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	3,75	45	3,75	9.360,00 €	9.360,00 €

Technician	2,75	31,25	2,84	6.201,00 €	6.406,25 €
TOTAL	**6,5**	**76,25**	**6,59**	**15.561,00 €**	**15.766,25 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	12	1	2.496,00 €	2.496,00 €
Researcher	0,75	9	0,75	1.872,00 €	1.872,00 €
TOTAL	**1,75**	**21**	**1,75**	**4.368,00 €**	**4.368,00 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	12	1	2.496,00 €	2.496,00 €
Researcher	1	12	1	2.496,00 €	2.496,00 €
TOTAL	**2**	**24**	**2**	**4.992,00 €**	**4.992,00 €**

P3: UMA

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	16,67	0,8335	8.300,00 €	8.300,00 €
Administrative	1	16,67	0,8335	3.750,00 €	3.750,00 €
TOTAL	**2**	**33,34**	**1,6667**	**12.050,00 €**	**12.050,00 €**

WP2: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO JULY 2023

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	5	100	5	25.000,00 €	25.000,00 €
TOTAL	**5**	**100**	**5**	**25.000,00 €**	**25.000,00 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	20	1	5.000,00 €	5.000,00 €
TOTAL	**1**	**20**	**1**	**5.000,00 €**	**5.000,00 €**

WP4: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO OCTOBER 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	6	120	6	30.000,00 €	30.000,00 €
TOTAL	**6**	**120**	**6**	**30.000,00 €**	**30.000,00 €**

WP5: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2024 TO FEBRUARY 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	6	120	6	30.000,00 €	30.000,00 €
Technician	2	40	2	8.000,00 €	8.000,00 €
TOTAL	**8**	**160**	**8**	**38.000,00 €**	**38.000,00 €**

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	2	43,6	2	10.900,00 €	10.900,00 €
TOTAL	**2**	**43,6**	**2**	**10.900,00 €**	**10.900,00 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	20	1	5.000,00 €	5.000,00 €
TOTAL	**1**	**20**	**1**	**5.000,00 €**	**5.000,00 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	20	1	5.000,00 €	5.000,00 €
TOTAL	**1**	**20**	**1**	**5.000,00 €**	**5.000,00 €**

P4: ESHA

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	2	31,62	1,73	10.604,00 €	15.251,60 €
TOTAL	**2**	**31,62**	**1,73**	**10.604,00 €**	**15.251,60 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	18,31	1	5.302,00 €	6.616,04 €
TOTAL	**1**	**18,31**	**1**	**5.302,00 €**	**6.616,04 €**

WP5: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2024 TO FEBRUARY 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	19,19	1,05	5.302,00 €	7.816,88 €
TOTAL	**1**	**19,19**	**1,05**	**5.302,00 €**	**7.816,88 €**

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	4	6,31	0,34	21.208,00 €	3.364,94 €
TOTAL	**4**	**6,31**	**0,34**	**21.208,00 €**	**3.364,94 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	2	18,51	1,01	10.604,00 €	8.119,87 €
TOTAL	**2**	**18,51**	**1,01**	**10.604,00 €**	**8.119,87 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	6	210,26	11,5	31.812,00 €	71.375,34 €
TOTAL	**6**	**210,26**	**11,5**	**31.812,00 €**	**71.375,34 €**

P5: ECSO

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	27,5	1,29	5.500,00 €	10.242,44 €
Administrative	1	15	0,71	7.300,00 €	6.015,38 €
TOTAL	**2**	**42,5**	**2**	**12.800,00 €**	**16.257,82 €**

WP2: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO JULY 2023

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	2	51	2,36	11.000,00 €	16.286,00 €
TOTAL	**2**	**51**	**2,36**	**11.000,00 €**	**16.286,00 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	3	64	3	16.500,00 €	15.832,00 €
TOTAL	**3**	**64**	**3**	**16.500,00 €**	**15.832,00 €**

WP5: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2024 TO FEBRUARY 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	2	43	1,99	11.000,00 €	13.728,56 €
TOTAL	**2**	**43**	**1,99**	**11.000,00 €**	**13.728,56 €**

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	5	104,5	5	27.500,00 €	32.383,96 €
TOTAL	**5**	**104,5**	**5**	**27.500,00 €**	**32.383,96 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	4	83	4	22.000,00 €	24.093,35 €
TOTAL	**4**	**83**	**4**	**22.000,00 €**	**24.093,35 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	5	105	4,91	27.500,00 €	24.689,08 €
TOTAL	**5**	**105**	**4,91**	**27.500,00 €**	**24.689,08 €**

P6: AVANZI

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMEBR 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	1	21	1,09	8.320,00 €	6.055,40 €
Administrative	1	34,3	1,85	3.200,00 €	6.239,12 €
TOTAL	**2**	**55,3**	**2,95**	**12.270,00 €**	**12.294,52 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	16	0,84	4.320,00 €	2.707,45 €
TOTAL	**1**	**16**	**0,84**	4.320,00 €	2.707,45 €

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	25	1,31	5.320,00 €	5.864,96 €
TOTAL	**1**	**25**	**1,31**	**5.320,00 €**	**5.864,96 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	8	179	8,22	34.560,00 €	34.580,35 €
TOTAL	**8**	**179**	**8,22**	**34.560,00 €**	**34.580,35 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	27	1,24	4.320,00 €	4.359,57 €
TOTAL	**1**	**27**	**1,24**	**4.320,00 €**	**4.359,57 €**

P7: CGI

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Manager	2	49	2,33	7.000,00 €	9.064,16 €
TOTAL	**2**	**49**	**2,33**	**7.000,00 €**	**9.064,16 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Technician	2	42	2	5.200,00 €	7.793,46 €
TOTAL	**2**	**42**	**2**	**5.200,00 €**	**7.793,46 €**

WP4: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO OCTOBER 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Technician	8	168	8	20.800,00 €	31.632,31 €
TOTAL	**8**	**168**	**8**	**20.800,00 €**	**31.632,31 €**

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Technician	2	42	2	5.200,00 €	7.951,59 €
TOTAL	**2**	**42**	**2**	**5.200,00 €**	**7.951,59 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Technician	1	21	1	2.600,00 €	3.954,96 €
TOTAL	**1**	**21**	**1**	**2.600,00 €**	**3.954,96 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Technician	1	21	1	2.600,00 €	3.501,96 €
TOTAL	**1**	**21**	**1**	**2.600,00 €**	**3.501,95 €**

P8: TLU

WP1: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Amministrative	2	49	2,3	6.000,00 €	12.833,84 €
TOTAL	**2**	**49**	**2,3**	**6.000,00 €**	**12.833,84 €**

WP2: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO JULY 2023

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	21	1	3.000,00 €	3.054,3 €
TOTAL	**1**	**21**	**1**	**3.000,00 €**	**3.054,3 €**

WP3: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM MAY 2023 TO JUNE 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	14	256	12,1	42.000,00 €	25.175,11 €
TOTAL	**14**	**256**	**12,1**	**42.000,00 €**	**25.175,11 €**

WP4: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY TO OCTOBER 2024

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	21	1	3.000,00 €	5.398,98 €
TOTAL	**1**	**21**	**1**	**3.000,00 €**	**5.398,98 €**

WP5: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2024 TO FEBRUARY 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	3	83	4	11.000,00 €	11.100,85 €
TOTAL	**3**	**83**	**4**	**11.000,00 €**	**11.100,85 €**

WP6: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM OCTOBER 2024 TO NOVEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	2	80	3,8	6.000,00 €	11.450,00 €

TOTAL	**2**	**80**	**3,8**	**6.000,00 €**	**11.450,00 €**

WP7: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMBER 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	24	1	3.000,00 €	3.342,03 €
TOTAL	**1**	**24**	**1**	**3.000,00 €**	**3.342,03 €**

WP8: SUMMARY OF WORKING DAYS/PMs PER STAFF CATEGORY FROM JANUARY 2023 TO DECEMEBR 2025

STAFF CATEGORY	BUDGET (PMs)	DAYS REPORTED	PMs REPORTED	BUDGET (TOTAL COSTS)	ACTUAL COSTS INCURRED
Researcher	1	20	1	3.000,00 €	2.972,43 €
TOTAL	**1**	**20**	**1**	**3.000,00 €**	**2.972,43 €**

5.2 Annex 2: Detailed mapping of all data categories, tools, recipients and purposes

Categories of data subjects	Categories of personal data	Categories of NON personal data	Purpose of processing	Means of processing	Who is responsible for data collection and processing?	Recipients/Categories of recipients	General Description of Technical And Org. Security Measures
Teachers and school leaders participating in the SuperCyberKids project activities	Username, Country, Email SuperCyberKids Platform usage data: • user's Device's Internet Protocol address • pages of platform services visited • time and date of the visit • content used	N/A	Teachers' registration to and use of the SuperCyberKids platform	SuperCyberKids platform	GRIFO	GRIFO and SuperCyberKids project partners	Information available inside the privacy police accessible inside the SuperCyberKids platform. (https://platform.supercyberkids.eu/privacy-policy)

	• rating expressed • personal playlists • uploaded materials						
Teachers and School leaders participating in the SuperCyberKids project activities	Name and Surname, Country, Role (Teacher/Headteacher), email	N/A	Recruitment of data subjects for the purposes of evaluating the methodology .	Informed consent for participation in research and privacy consent in digital form, from participating teachers	CNR	SuperCyberKids project partners	Secure Server hosted inside CNR's facilities
Teachers and School leaders participating in the SuperCyberKids project activities	Name and Surname, Country, Role (Teacher/Headteacher), email	Date of the training activity	Demonstrate attendance in the pilot training activities	List of participants attending the training activities	SuperCyberKids project partners responsible for the pilot	SuperCyberKids project partners, European Funding Agency	Digital documents secured in a protected and secure digital space (e.g. the project Teams space).

Teachers participating in the SUPERCYBERKIDS project activities	Country, School Name, Taught Subject, Average age of the students	Anonymous questions assessing the perception and satisfaction of teachers with regard of their training on the use of SuperCyberKids resources. In particular: • Importance, urgency, confidence, and previous inclusion of cybersecurity topics in teaching • Strategies, challenges, and use of gamification as teaching approaches • Cybersecurity preparedness: How well the teacher feels	Pre/Post questionnaire evaluation of the perception and satisfaction of teacher with regard of their training on the use of SuperCyberKids resources	Self-Hosted Limesurvey Platform	AVANZI, CNR	SuperCyberKids project partners	Secure Server hosted inside CNR's facilities Data collected is anonymous and without any associations with participants' name and surnames

		prepared to incorporate cybersecurity • Training feedback: Most useful concepts, suggestions for improvement, and recommendation to other teachers					
Teachers participating in the SuperCyberKids project activities	Country, School Name, Subject Taught, Average age of the students	Anonymous questions on the satisfaction of teachers with regard of their use of the SuperCyberKids Platform and resources. In particular: • Anonymous students' response to SuperCyber	Questionnaire evaluation of the satisfaction of teacher with regard of their use of SuperCyberKids Platform and resources	Self-Hosted Limesurvey Platform	AVANZI, CNR	SuperCyberKids project partners	Secure Server hosted inside CNR's facilities Data collected is anonymous and without any associations with participants' name and surnames

		Kids resources and games • Quality and usefulness of SuperCyber Kids resources • General feedback with regards to challenges encountered and suggestions for improvement					
Teachers participating in the SuperCyber Kids project activities	All data from the user account in the platform is automatically associated with the form (username, email, and country of provenance)	A small questionnaire collecting teachers' feedback on their experience with regards to specific pilot activities and modules. In particular: Teacher Feedback: Teachers will have	Questionnaire collecting teachers' feedback to evaluate the quality of the resources	SuperCyberKids Platform	GRIFO, AVANZI	SuperCyberKids project partners	Information available inside the privacy police accessible inside the SuperCyberKids platform. (https://platform.supercyberkids.eu/privacy-policy)

		the possibility to rate the material, the interest of the students and if they will be using it in the future					
School leaders participating in the SuperCyber Kids project activities	School Name, Average age of the students	A questionnaire collecting headteachers' feedback on their experience with the implementation of the pilot activities. In particular: • Willingness to promote the SuperCyber Kids ecosystem • Feedback on the pilot experience • Information about the integration of the SuperCyber Kids activities	Anonymous questionnaire collecting headteachers' feedback with regards to their experience in the implementation of the pilot in their school and their willingness to promote the SuperCyberKids ecosystem and outputs to colleagues	Self-Hosted Limesurvey Platform	CNR, AVANZI	SuperCyberKids project partners	Secure Server hosted inside CNR's facilities

		into school curricula					
Teachers participating in the SuperCyberKids project activities	All data from the user account in the platform is automatically associated with the form (username, email, and country of provenance)	Quality rating expressed in a number of stars (points), average of ratings shown	Evaluation of the users' feedback on SuperCyberKids resources.	SuperCyberKids Platform	GRIFO	SuperCyberKids project partners	Information available inside the privacy police accessible inside the SuperCyberKids platform. (https://platform.supercyberkids.eu/privacy-policy)
Teachers participating in the SuperCyberKids project activities	All data from the user account in the platform is automatically associated with the form (username, email, and country of provenance)	Assessment of average students learning mediated by the teacher.	Pre/Post Evaluation of the average student learning using the teacher as a moderator. No personal data from students will be collected.	SuperCyberKids Platform	GRIFO, UMA	SuperCyberKids project partners	Information available inside the privacy police accessible inside the SuperCyberKids platform. (https://platform.supercyberkids.eu/privacy-policy)
Teachers and School leaders participating in the SuperCyberKids	Role, Subject Taught	Opinions expressed in a focus group and collected by means of an anonymous report	Focus group aimed at collecting participants insights on the implementation and impact of cybersecurity	Written report in a digital format	SuperCyberKids project partners involved in the piloting activities	SuperCyberKids project partners	The focus group will not be recorded. Feedback and insights will be collected in an anonymous report, that will refer participants only by

project activities			resources designed for children.				their role and subject taught.
Interviews to selected high-level stakeholders	Name, Surname, Role	Opinions on the project's relevance and sustainability	Interviews aimed at collecting feedback from a set of selected high-level stakeholders on the relevance and sustainability of the project	Written report in a digital format	AVANZI	SuperCyberKids project partners	Interviews will not be recorded.