Memorandum of Understanding

SuperCyberKids
Deliverable no D8.3

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

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Project ref. number	101087250
Project title	**SCK - SuperCyberKids**
Document title	Memorandum of Understanding
Document Type	Deliverable
Document version	<1, 29.09.2025>
Previous version(s)	<vn-1>
Planned date of delivery	<30.09.2025>
Language	English
Dissemination level	Public
Number of pages	10
Partner responsible	ESHA
Author(s)	Luca Laszlo, ESHA
With contributions by:	
Revised by:	Manuel Gentile, CNR
Abstract	This deliverable explains the objectives and development process of the MoU, outlines its content, and highlights its expected impact on European education and digital literacy policy. It also defines next steps, including stakeholder engagement at the Final Conference (D8.2), where signatures will be formally invited.
Keywords	Cybersecurity education; Memorandum of understanding; SuperCyberKids
DOI	https://doi.org/10.17471/54033
How to cite	Laszlo, L., (2025). Memorandum of Understanding. Deliverable 8.3 - SuperCyberKids project (ERASMUS-EDU-2022-PIFORWARD - ERASMUS-LS - Project No. 101087250). DOI: https://doi.org/10.17471/54033

Internal project peer review process

Approved by		
Manuel Gentile	Project Coordinator (CNR-ITD)	30/9/2025

Table of Contents

1 Executive Summary

The SuperCyberKids (SCK) project aims to create a sustainable impact on educational innovation by fostering safer digital environments for children. It does so by equipping schools, parents, and policymakers with innovative tools, resources, and methods for educational initiatives dedicated to prevention of, and response to, cyber threats. To ensure the long-term uptake and sustainability of project results, Deliverable D8.3 presents a Memorandum of Understanding (MoU) for relevant stakeholders.

The MoU formalises the commitment of schools, ministries, industry actors, parent associations, and civil society organisations to continue collaborating with SCK beyond the project's lifetime. It provides a common framework for the use, promotion, and further development of SCK outputs, including:

- Educational guidelines and handbooks.
- Localised educational games (NABBOVALDO and SPOOFY).
- The user platform and enactment package.
- Policy roadmaps and recommendations.

This deliverable explains the objectives and development process of the MoU, outlines its content, and highlights its expected impact on European education and digital literacy policy. It also defines next steps, including stakeholder engagement at the Final Conference (D8.2), where signatures will be formally invited.
The annex to this document includes the generic MoU text, designed to be concise and adaptable, encouraging diverse organisations to sign and commit to supporting the SCK initiative.

2 Introduction

The SuperCyberKids (SCK) project develops innovative tools and practices to enhance digital literacy and cybersecurity awareness among children, parents, and educators. An evaluation of the SCK project, undertaken together with its main stakeholders, has confirmed its positive impact. While project activities produce guidelines, educational games, and a gamification platform, sustainability requires ongoing cooperation among stakeholders beyond the project lifetime.

The Memorandum of Understanding (MoU) presented in this deliverable is designed as a lightweight but formal instrument to support continued collaboration. It aligns with the project's exploitation plan and roadmap (D8.1) and complements the dissemination and communication activities (R8.1.2). The MoU will be promoted and signed during the Final Conference (D8.2) and will remain open to additional stakeholders afterwards.

3 Objectives of the MoU

The MoU establishes a shared commitment to:

- Support long-term use of SCK results such as the guidelines, games, gamification platform, and enactment package.
- Promote adoption in schools and communities to strengthen children's digital resilience.
- Facilitate policy uptake by aligning outputs with digital education strategies at national and EU levels.

- Encourage stakeholder collaboration among schools, parent associations, policymakers, industry, and civil society.
- Support sustainability by providing a framework for voluntary cooperation after the project ends.

Alignment with Project Objectives–the MoU was conceived as a sustainability instrument, directly linked to:

- The Exploitation Plan, which identifies key assets (guidelines, games, gamification platform, enactment package).
- The roadmap (D8.1), which outlines pathways for long-term uptake and policy alignment.
- The Dissemination and Communication Plan (R8.1.2), which provides channels to promote and support signature of the MoU.

Dissemination of the MoU will take place through the project website, newsletters, social media, and the Final Conference (D8.2).

4 Content of the MoU

The MoU is a concise, non-binding agreement that establishes a framework for cooperation between stakeholders committed to promoting the sustainable use of SuperCyberKids results. Its content reflects the project's exploitation vision while remaining generic enough for diverse organisations to sign.

It reaffirms the shared mission of supporting children, parents, and educators in building resilience against cyber threats and invites stakeholders from education, policy, research, industry, and civil society to acknowledge the value of SCK outputs formally.

The scope of the MoU encompasses the uptake of project assets, including pedagogical guidelines, educational games, a gamification platform, an enactment package, and a handbook. Commitments include promoting awareness, applying tools, sharing feedback, and supporting collaboration. Governance is informal, and the MoU remains valid indefinitely unless otherwise agreed among the parties involved.

5 Expected impact and next steps

The MoU is expected to generate impact at both policy and school levels.

Policy-Level Impact–The MoU supports the European Digital Education Action Plan (2021–2027) and EU/national strategies through integration of digital resilience into curricula, alignment with cybersecurity policies, and strengthening of multi-stakeholder governance.

Institutional and School-Level Impact–For schools, the MoU makes available practical tools such as guidelines, games, the gamification platform, and an enactment package. By signing, schools show commitment to student well-being and gain visibility as part of a European cybersecurity-active community.

Long-Term Sustainability–The MoU anchors SCK outputs in ongoing dissemination, networking, and policy advocacy.

The MoU represents an important step towards ensuring the sustainability of SuperCyberKids. Its impact will depend on:

- Promotion and awareness-raising through dissemination channels.
- Stakeholder engagement across education, policy, industry, and civil society.

- Integration with the exploitation roadmap and final conference outcomes.
- Expansion of the community of practice by welcoming new signatories.
- Policy advocacy linking practice with structural support.

The MoU will act as both a symbolic and practical instrument for collaboration.

6 Policy Brief: Cybersecurity Education for Children in Europe

This policy brief has been developed as a practical tool to support the implementation of the Memorandum of Understanding (MoU) on strengthening digital education in Europe. Its purpose is to highlight why cybersecurity education for children matters, where current gaps exist, and how different stakeholders — from EU institutions to national authorities, schools, and local communities — can contribute to a safer, more resilient digital learning environment.

For potential signatories of the MoU, the brief serves as both a reference and a call to action: it shows how their engagement can help build a more cybersecurity-aware education landscape, where children are equipped not only to avoid digital risks but also to respond effectively when challenges arise. By setting out key messages, evidence, and concrete actions at different levels, the brief provides a common basis for coordinated strategies and can form the foundation of forthcoming SuperCyberKids stakeholder guidelines.

6.1 Key messages

- Children are growing up online from an early age, but schools are not yet systematically preparing them to navigate digital risks.
- Cybersecurity is a life skill for all, not just a technical subject for a few.
- Schools and teachers are on the frontline in developing these skills but lack the necessary tools, training, and resources.
- Game-based learning is an effective and inclusive way to teach children about digital safety.
- Systemic action is needed: without EU, national, and local policy coordination, progress will remain fragmented and unequal.
- Risk cannot be eliminated — but it can be mitigated. By equipping children with competencies, we reduce their exposure to harm and empower them to respond effectively when incidents occur.

6.2 How we know it

Children's digital immersion is a reality across Europe. Research shows that children as young as eight are active online, yet early education on safe and responsible internet use remains patchy. Many schools still prioritise access to devices and connectivity over online safety and resilience.

European data confirms this gap. The *Eurydice Digital Education at School in Europe Report (2019)* found that only one in three schools has a digital development plan, and very few explicitly address cybersecurity. The *EU Kids Online 2020* survey documented increasing exposure of children to risks such as bullying, scams, grooming, and privacy breaches.

The *Digital Education Action Plan 2021–2027 (COM(2020)624)* highlights the need for innovative pedagogies to develop digital competences. However, even with strong frameworks, the reality is that not all online risks can be prevented. This aligns with the *EU Strategy on the Rights of the Child*

(COM(2021)142), which calls for measures that **minimise harm** and strengthen children's ability to cope when risks materialise.

SuperCyberKids pilots in Italy, Estonia, Germany, and EU-wide confirmed this principle:

- Children became more aware of threats and more resilient in handling them.
- Teachers gained tools to guide children not only in prevention, but also in coping strategies when risks could not be avoided.
- School leaders found that embedding cybersecurity in school development plans helped reduce the negative impact of incidents, creating safer digital learning environments.

6.3 What the different levels can do

6.3.1 At EU level

The European Union has already placed digital competence at the heart of its *Digital Education Action Plan (2021–2027)* and the *EU Cybersecurity Strategy for the Digital Decade*. However, cybersecurity education for children remains underdeveloped in these frameworks. To close the gap, the EU should:

Strengthen the policy framework by updating the *Recommendation on Key Competences for Lifelong Learning* to explicitly include online safety, privacy awareness, and cyber resilience as basic competences. This would provide a clear mandate for Member States to integrate cybersecurity into their educational curricula.

Develop standard guidelines for cybersecurity education in collaboration with ENISA and ECSO Youth4Cyber, ensuring consistency in scope, age appropriateness, and learning outcomes. EU-level guidance would help avoid fragmentation and ensure that all children in Europe benefit from a comparable standard of protection.

Fund innovation and upscaling of open-access, game-based resources through Erasmus+ and Horizon Europe. Such investment would ensure that cost and language are not barriers to access, and that even small or rural schools can benefit from high-quality educational ecosystems.

Facilitate cross-border knowledge exchange by embedding cybersecurity topics into platforms such as eTwinning, the School Education Gateway, and the European Education Area. This would enable schools and teachers to share best practices, build peer learning networks, and disseminate innovation more rapidly.

6.3.2 At national level

Member States play the key role in curriculum development, teacher training, and quality assurance. National action is essential to turn EU guidance into a classroom reality. To achieve this, governments should:

Embed cybersecurity systematically into curricula at primary and lower-secondary levels, ensuring continuity between digital literacy and wider civic competences. Cybersecurity should be treated not as an optional extra, but as a fundamental building block of education for all children.

Mandate teacher professional development in cybersecurity education. Teachers across subjects — not just ICT specialists — should be trained to address online safety, risk mitigation, and resilience. National CPD frameworks should include clear learning objectives on these themes.

Support localisation and cultural adaptation of EU-funded resources, ensuring that educational games and guidelines are available in all national languages and reflect the diverse realities of learners. This avoids duplication of effort, while enabling inclusivity.

Establish national support structures such as observatories, centres of excellence, or digital safety helplines. These can provide schools with expert advice, monitor progress, and ensure that incidents are addressed not only reactively but also through systemic learning.

Align cybersecurity education with child rights and inclusion strategies, ensuring vulnerable groups are not left behind. This responds directly to the *EU Strategy on the Rights of the Child* and helps mitigate risks for those most exposed.

6.3.3 At local / school leadership level

Schools and their leaders are at the frontline of change. Digital innovation policies can only succeed if they are effectively implemented in everyday practice within school communities. To this end, school leaders and local authorities should:

Adopt whole-school approaches to cybersecurity, embedding it within school development strategies alongside digitalisation, wellbeing, and safeguarding. This signals to teachers, parents and pupils that online safety is a shared responsibility.

Provide ongoing training and peer support for teachers, enabling them to acquire the knowledge and skills, and to integrate cybersecurity into diverse subjects and everyday classroom practices. Local networks can amplify impact by sharing resources and experiences across schools.

Engage parents as active partners—awareness sessions, workshops, and joint activities can strengthen families' ability to mitigate risks at home and complement learning at school. Involving parents also fosters trust and ensures that children receive consistent messages across different environments.

Develop local partnerships with NGOs, libraries, community groups, and technology providers. These collaborations can provide resources, expertise, and real-world relevance, while reinforcing the notion that digital safety is a collective responsibility.

Encourage peer learning among school leaders—bodies such as ESHA (https://esha.org/) can support head teachers in exchanging successful practices, learning from challenges, and scaling up what works. School leaders, as local decision makers, have the power to shape systemic change within and beyond their institutions.

7 Annex – Memorandum of Understanding

Between Stakeholders Committed to the Sustainability of the SuperCyberKids Project Results and the SuperCyberKids consortium

1. Purpose

The purpose of this MoU is to establish a framework for continued cooperation among stakeholders committed to promoting digital literacy, resilience, and cybersecurity awareness among children, parents, and educators. It supports the sustainability of the SuperCyberKids (SCK) project (Project No. 101087250) by encouraging use, dissemination, and further development of its outputs. The

2. Scope

This MoU covers the adoption and promotion of SCK resources, including guidelines, educational games, the gamification platform, enactment package, and policy recommendations. It is non-binding and open to any organisation committed to long-term sustainability of these results.

3. Parties

Eligible signatories include schools, teacher training institutions, parent associations, policy makers, NGOs, research organisations, and private-sector actors to express their commitment to the SuperCyberKids project. The project consortium is represented by its coordinator, Manuel Gentile.

4. Commitments

By signing, the eligible party expresses their intention to:

- Promote awareness and use of SCK resources.
- Share good practices and feedback.
- Support collaboration between stakeholder groups.
- Contribute to a European culture of safe digital engagement for children.

The Parties commit to implementing this Memorandum in line with fundamental European principles of inclusivity, non-discrimination, respect for diversity, and openness, including the use of Creative Commons licensing where appropriate.

5. Governance

The MoU does not establish a formal governance structure. Cooperation will be supported through the project website (www.supercyberkids.eu), events, and informal coordination among signatories.

6. Duration

This MoU enters into effect upon signature and remains valid indefinitely, unless a signatory withdraws by written notice.

7. Signatures

The undersigned agree to the terms of this MoU and commit to supporting the sustainability and promotion of SuperCyberKids results.

| Organisation | Representative | Position | Date | Signature |