



SuperCyberKids: A Lasting Legacy for Safer Digital Futures

As we approach the end of the project's funded period this December, we close one chapter but open another, long-lasting one.

Over the past years, the project has grown into a living ecosystem of tools, knowledge, and shared commitment around safer and more meaningful digital experiences for children and young people. While the formal financing period is coming to a close, the resources created through the project will remain fully available, actively maintained, and ready to be used by schools, organisations, educators, and families across Europe and beyond.

At the centre of this sustainability effort is the [SuperCyberKids platform](#), which will continue to provide open access to all project resources. The platform brings together educational materials, interactive tools, and practical guidance designed to help schools address cybersecurity and digital wellbeing in age-appropriate and engaging ways. New users can continue to register and explore the platform using the invitation code **2047Sup3r!**, ensuring that access remains open after the funding period.

SuperCyberKids is specifically designed for **children aged 8 to 13**, but the platform itself is intended to be used **by educators in classroom or school-based settings**, rather than by individual children independently. This design choice reflects a strong commitment to **data protection, child safety, and responsible digital practices**, ensuring that learning activities are facilitated by teachers and schools within secure and supervised environments. To support broad accessibility across Europe, the platform and its core resources are available in **English, Italian, Estonian, and German**, enabling use in diverse educational contexts.

A key strength of SuperCyberKids lies in the **breadth and depth of its outputs**, which have been designed with adaption and reuse in mind. so they can be embedded more easily into everyday educational practice. The project established a strong evidence base through the SuperCyberKids Learning **Framework**, supported by extensive mapping of existing cybersecurity education initiatives and digital competence frameworks across Europe. This foundation helps schools understand not only *what* to teach, but *why* and *how* cybersecurity education fits within broader learning goals for children aged 8 to 13.

Building on this framework, the project developed **clear guidelines for integrating SuperCyberKids into school curricula**. These resources support school leaders and educators in making cybersecurity a pillar in young people's education in a realistic and sustainable way whether through existing subjects, cross-curricular approaches, or whole-school strategies—rather than treating it as a standalone or one-off activity.

SuperCyberKids now makes available **fully adapted and localised educational games**. These include *Nabbovaldo* and *Spoofy*, which translate complex cybersecurity concepts into playful, meaningful learning experiences for children. Alongside further, extended versions of these games, the project has produced guidance for game designers and developers, making it easier for others to adapt or create new educational games using a child-centred, pedagogically sound approach.

To support real-world implementation, the project produced a **game oriented platform - and related back-end tools- for teachers**, as well as an enactment package based on pilot use cases. Together, these resources help schools and education organisations move from theory to practice, offering concrete examples of how SuperCyberKids can be used in classrooms and learning communities.

Equally important is the project's focus on **long-term impact and sustainability**. SuperCyberKids has produced a **handbook of good practices** for cybersecurity education in schools, a **roadmap for extending the ecosystem**, and a **Memorandum of Understanding (MoU)** that allows schools, organisations, and other stakeholders to link up with SuperCyberKids formally express their support and non-binding commitment to using and promoting the project's resources.

Alongside the MoU, the project has also developed a set of **policy recommendations**, which translate the project's findings into clear, actionable guidance for policymakers and education authorities. These recommendations highlight how cybersecurity education for children can be better supported through policy, curriculum frameworks, and cross-sector collaboration. While the MoU expresses institutional commitment to using the resources

in practice, the policy recommendations inform decision-making at system level and support longer-term structural change.

In SuperCyberKids, sustainability has always meant more than continued access to online material.. It means enabling educators to continue using resources with confidence, supporting schools in embedding digital safety into everyday learning, and ensuring that children benefit from consistent, thoughtful approaches to cybersecurity education. Through use of the platform and its practical resources, signing the Memorandum of Understanding, and reference to the accompanying policy recommendations, the impact of SuperCyberKids will continue into the future.

We warmly invite you to explore the platform, share the resources with your educational community, and join us by expressing your support through the **Memorandum of Understanding**.

Find all project outputs on the project website: <https://www.supercyberkids.eu/>