



**SUPER CYBER
KIDS**



**SUPER CYBER
KIDS**

SuperCyberKids

Summary guidelines for teachers and professional educators



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.

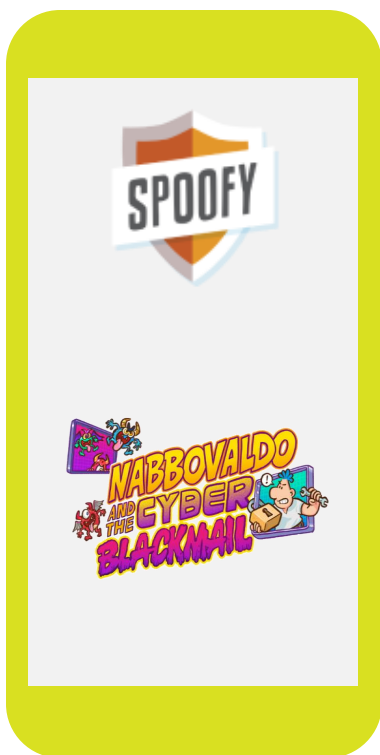
Please be aware of the following



- Please take into account that this document is not the only guidance document for schools and teachers. Other guidance material is also provided by ESHA, ECSO or Erasmus+ .

Introduction

SuperCyberKids aims at helping students recognise and respond to cyber threats, understand the importance of protecting personal information, and develop responsible online behaviours.



This set of guidelines is designed to assist education professionals in utilising a dedicated platform to educate kids about cyber safety through engaging games, educational materials, and interactive resources.



By integrating these tools into the classroom, teachers can create a dynamic and interactive learning environment that not only informs but also empowers pupils to protect themselves online.

These guidelines aim to help teachers gain time in the implementation of SuperCyberKids

What teachers can do with the SuperCyberKids platform



Teachers can search and browse the teaching resources included in the SuperCyberKids digital platform, that is, lesson plans, games and quizzes. The platform offers a database of lesson plans, games and learning resources on cybersecurity, which can be searched by competencies, age level, type of resource.



Teachers can use the SuperCyberKids digital platform to easily decide which games they can use in the classroom as supporting tools for the curricula on cybersecurity.



Teachers can upload their own resources on cybersecurity in addition to those already present on the platform. The content available on the platform can be collected by teachers in personalised lists (or playlists), or they can use off-the-shelf lists of content recommended by SuperCyberKids.



Teachers can leave comments and recommendations on the learning resources (rating system), thus enriching the database of resources on cybersecurity.



Content Variables

Tailor content to age, setting, resources, game format (homework, individual, group), prior knowledge, and ensure it serves multiple educational purposes (demonstration, training, motivation).



Educational Objectives / Learning Outcomes

Define student knowledge, skills, and attitudes post-lesson, using the SuperCyberKids EU framework to align with modules like Cyber Attacks, Data Privacy, Frauds, Safety, and more.



Safety Measures

Integrate the safety measures and preventive techniques from the SuperCyberKids Learning Framework into the game-based learning environment.



Lesson Activities

Use interactive methods like game-based learning to boost engagement while ensuring activities align with educational objectives.



Assimilation of Existing Content

Understand the educational objectives, capabilities, and limitations of existing content like the Spoofy and Nabbovaldo games, and integrate it seamlessly into the lesson plan as a complementary tool.



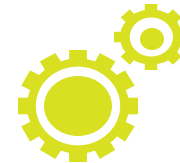
Student Engagement

Adapt the interaction pattern (Teacher Monitored Use, Group Play, etc.) to maximise student engagement and learning, ensuring alignment with the framework's objectives.



Feedback and Adaption

Continuously monitor student progress and adapt the teaching strategy as needed. This should include formative assessments and could be facilitated by in-game analytics.



Assessment and Metrics (Indicators)

Use formative indicators (engagement, participation, feedback) and summative indicators (quiz scores, assignments, application of concepts) to assess learning, while considering the benefits and limitations of in-game and out-of-game assessments.



Review and Adaptation

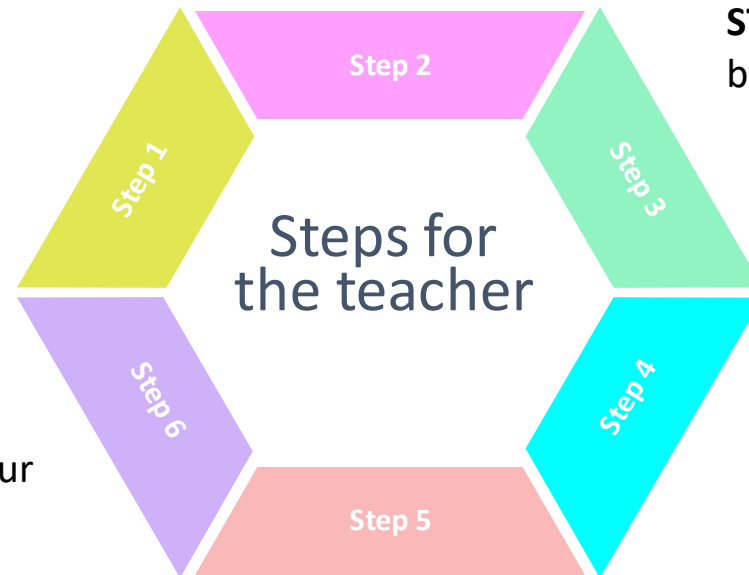
Analyze lesson success based on objectives and indicators, then adjust future lessons using this analysis and student feedback.

Everything you need to know before classroom activity in the classroom

STEP 2: Run the initial Assessment to define the learning needs of the class.

STEP 1: Accessing the platform. Once you fill in the registration form using the invitation code, you will get an automated email to the registered address with login details (Username and Password).

STEP 3: Search the platform's database for resources by competencies, age level, type.



STEP 4: Use the learning resources (lesson plans, links to games, documents, video clips) to run activities in the classroom. **Create** your own personalised **playlist** of resources

STEP 6: Provide feedback on your experience.

STEP 5: Run the final assessment to measure learning progress.

Navigate the SuperCyberKids ecosystem

- Map of the 18 modules that have been prepared and approved by SuperCyberKids
- The map of the modules has been designed to look like a computer motherboard. It is divided into three areas, each of different colour:
 - Technical Skills (green)
 - Social Skills (blue)
 - Integrated Skills (red).

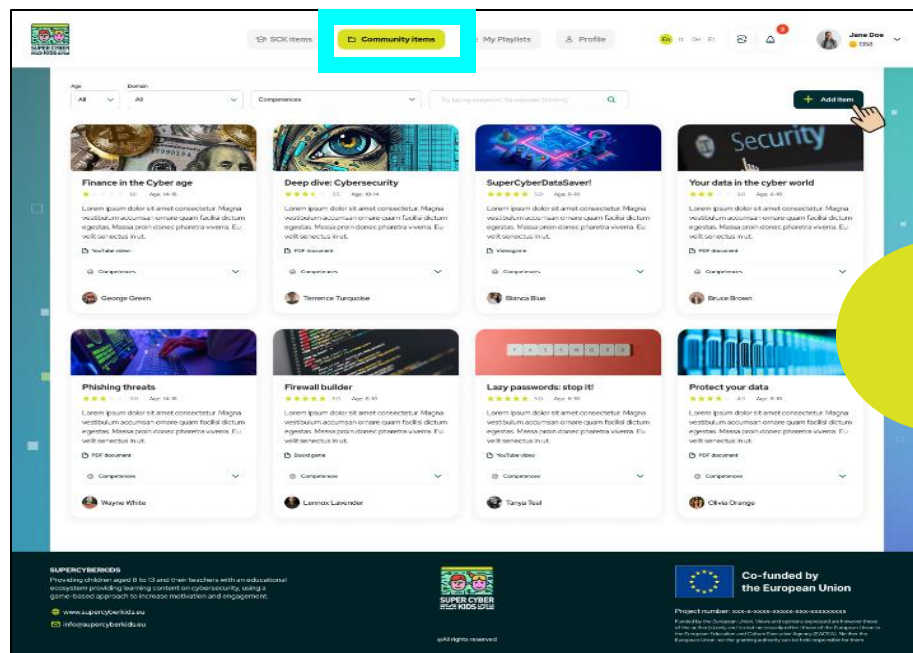


Top Menu

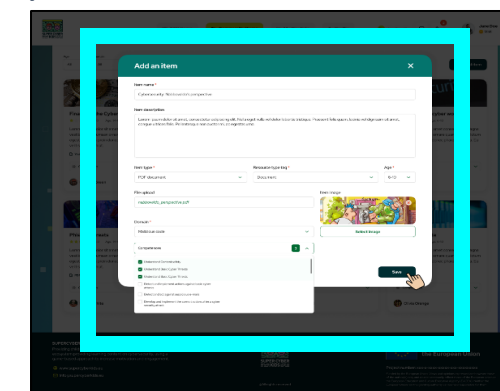
- Platform Items
- Community Items
- My Playlist
- Profile
- Search
- Knowledge test

Navigate the SuperCyberKids ecosystem

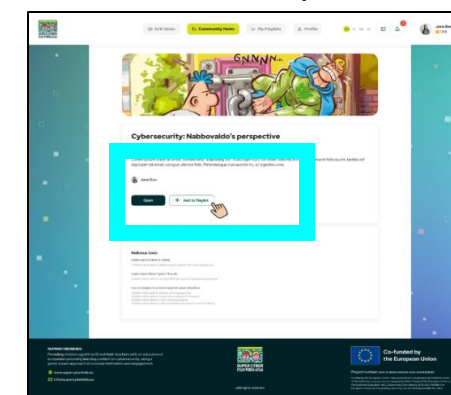
How to add an Item to the community items repository?



Community items



How to add an item to a personal playlist?



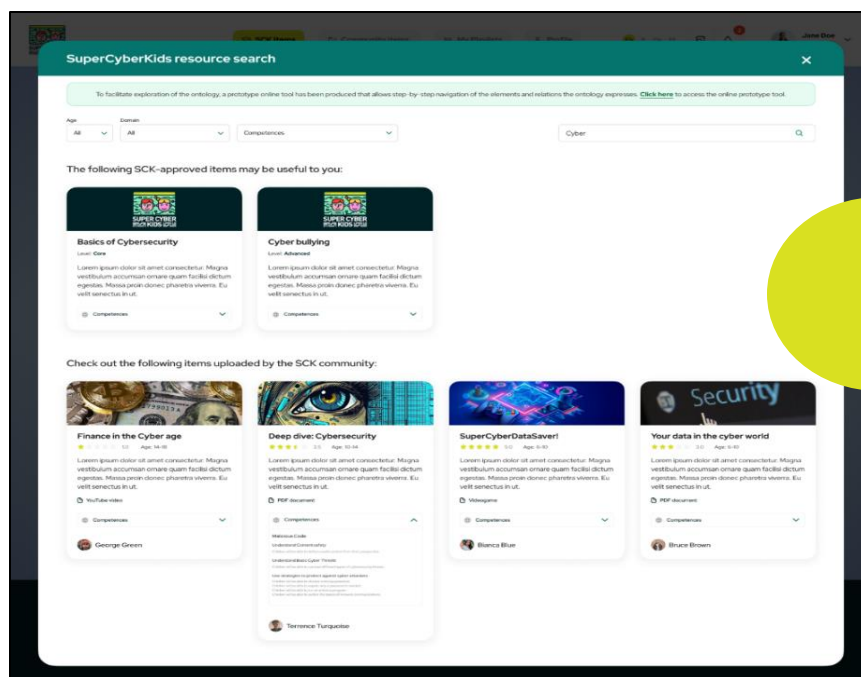
This area of the platform is a common repository of all resources suggested or uploaded by users (teachers). It contains all the items suggested, uploaded and catalogued by users and is visible to all users registered on the platform.



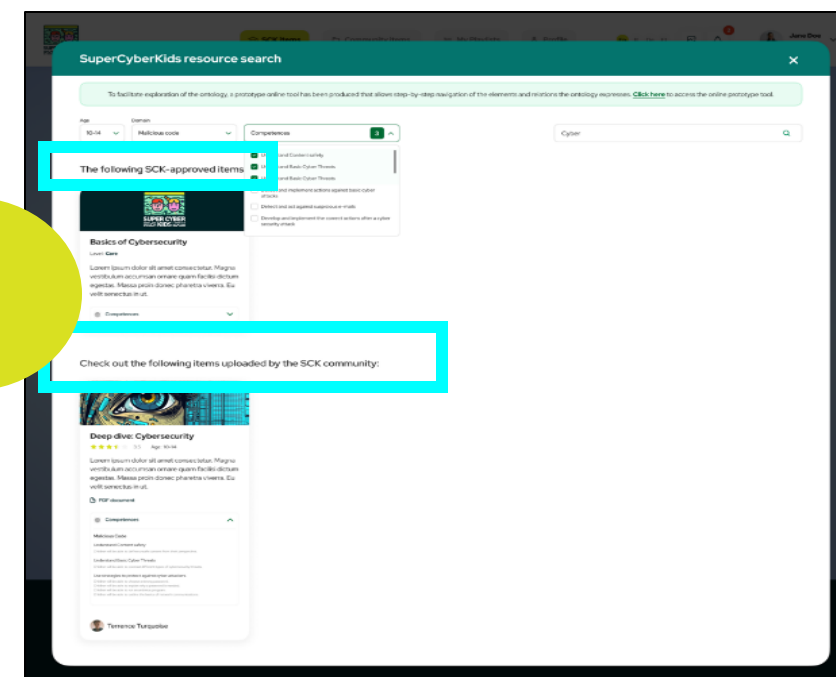
Navigate the SuperCyberKids ecosystem



You can use the Search function to retrieve learning resources from both areas of the platform: the set of SuperCyberKids-produced modules, and the collection of items suggested or uploaded by the community. Items at the top of the results page with the project logo are from the module-based area of the platform, while Community proposed items are displayed underneath.



Search Function



Co-funded by
the European Union

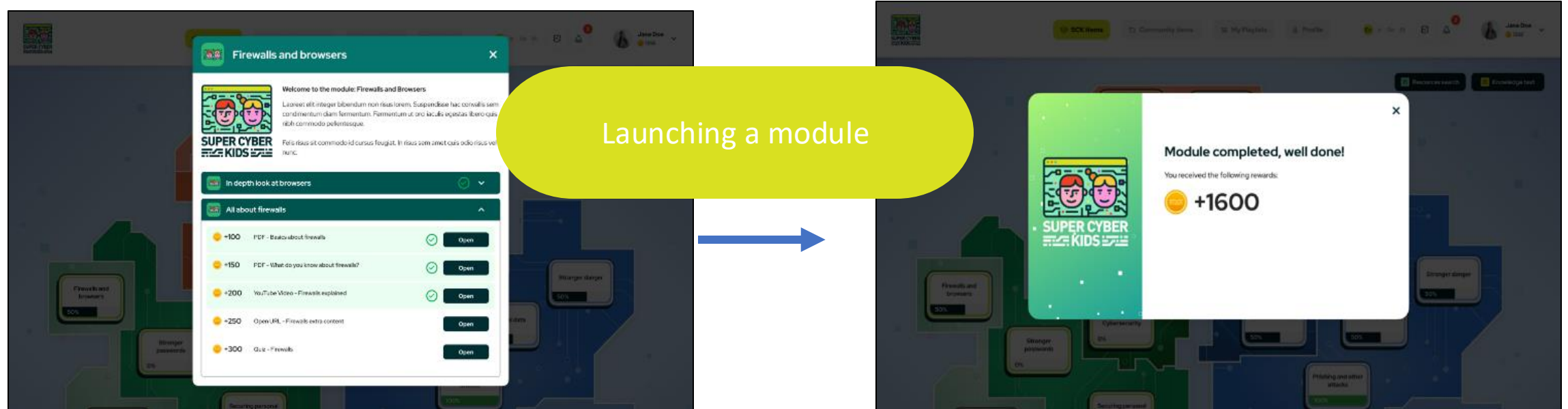
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for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



Navigate the SuperCyberKids ecosystem



When a user clicks on one of the 18 modules in the navigation page (in this example the user has selected the module “Firewalls and browsers”), a window opens showing the content of the module: this can be a lesson plan, a document to download, a quiz to test knowledge, or a link to a game. Opening each item, the user gains points that make up the final score. When all the items in the module have been opened, and, in case of a quiz, the quiz has been passed, the user is shown this window with the final score for that module



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.





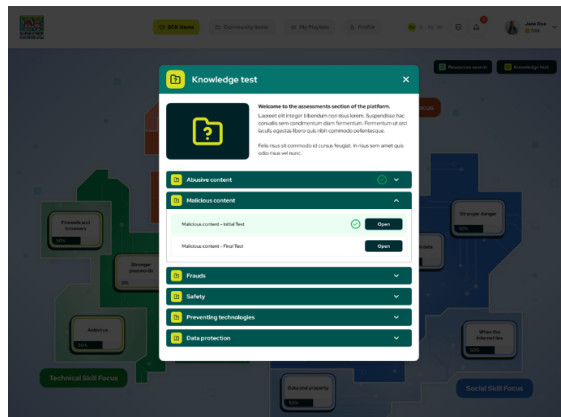
Navigate the SuperCyberKids ecosystem



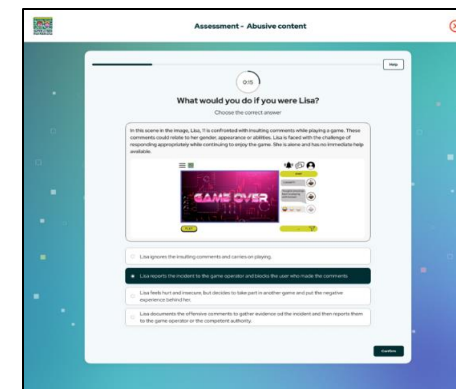
Initial and final assessments are available so you can identify the whole class's starting level of knowledge about cybersecurity topics (initial test) and how this level has progressed after learning activities (final test). These assessments cover six general areas of cybersecurity:

- Malicious Code
- Frauds
- Preventing Technologies
- Abusive Content
- Data Privacy & Data Awareness
- Safety.

At the end of each test, you will receive feedback on how many questions the class has answered correctly. You can identify which areas require more in-depth study.



Knowledge Test



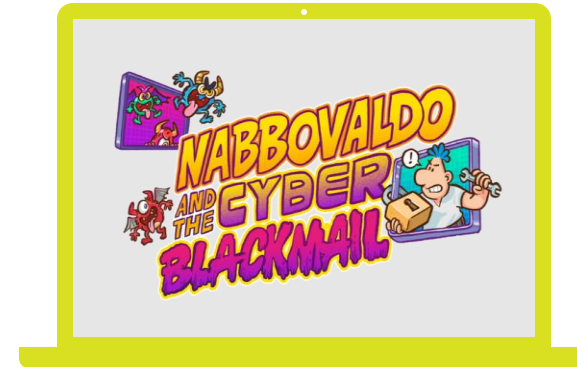
Co-funded by
the European Union

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.

The games in the SuperCyberKids ecosystem



Spoofy is a free, educational cybersecurity game for children that teaches internet safety, online behavior, and smart device issues. It features fun scenarios where players collect cyber-pets and solve problems in five worlds. Younger children can play with an adult, while older kids can tackle more complex challenges. The game encourages problem-solving, collecting items, and earning rewards like cyber-pets.



"Nabbovaldo and the Cyber Blackmail" is a game for children aged 11-14, designed to improve digital literacy and promote good online practices. It can be played solo or in the classroom to complement lessons. The game features a hybrid structure where players can follow a set path or explore freely, solving IT challenges in the city of Internetopoli through mini-games. Nabbovaldo encounters new characters who assist in overcoming cyber threats.

Implementation steps

- For the implementation of SuperCyberKids and its integration in the curriculum in the classroom, we recommend teachers to select for the first learning session the following module: “basics of cybersecurity”. The following teaching and learning approaches defined in 4 weeks are well established and can serve as an inspiration for your work.

Week 1

Introduction to Cybersecurity Threats and Unsafe Content

- Objectives:** Students will be able to define unsafe content from their perspective & Students will be able to contrast different types of cybersecurity threats.
- Activities:** Discussions on what constitutes unsafe content online. ; Introduction to various threats such as malware, phishing, and social engineering. ; Comparison and analysis of different cybersecurity threats through examples and case studies.

Week 2

Password Security

- Objectives:** Students will be able to choose a strong password & Students will be able to explain why a password is needed.
- Activities:** Guidelines for creating strong passwords ; Practical exercises on password strength ; Discussions on the importance of password protection.;

Real-world examples of data breaches to illustrate the need for strong

passwords.

Week 3

Antivirus Programmes

- Objectives:** Students will be able to run an antivirus programme
- Activities:** Introduction to antivirus software.; Hands-on practice in scanning and identifying potential threats. ; Discussion on the role of antivirus programmes in maintaining cybersecurity.

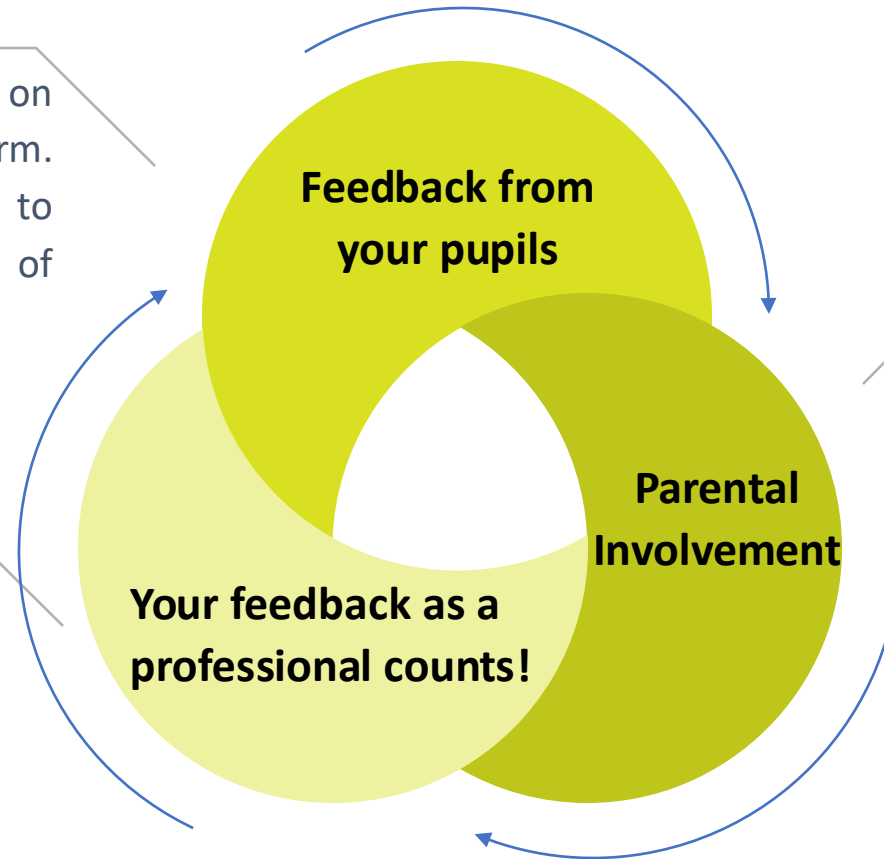
Week 4

Basics of Network Communications

- Objectives:** Students will be able to outline the basics of network communications.
- Activities:** Understanding how data travels across networks. ; Fundamentals of protocols and communication channels. ; Practical exercises on tracing data paths and understanding network components.

Gather feedback from students on their experience with the platform. Make necessary adjustments to improve the effectiveness of gamified activities.

You also have access to a feedback form where you can comment on the platform, send remarks, questions and suggestions. Your operational experience and expertise are important for us to develop the platform and ensure it is aligned with your needs.



Keep parents informed about the topics being covered and the resources being used. Home Activities: Suggest activities that parents can do with their children to reinforce learning at home.