Co-funded by the European Union

Project Nr. 2023-1-AT01-KA220-SCH-000166888

EnCycLEd

Enhancing Cybersecurity Literacy in Education

# PILOTING PROGRAM GUIDE FOR EDUCATION INSTITUTIONS

## Ukrainian Academy of Cyber Security

# EnCycLEd

Co-funded by
the European Union

## PROJECT'S COORDINATOR

**Leopold-Franzens-Universität**
Innsbruck

*www.uibk.ac.at*

## PROJECT'S PARTNERS

**University of Macedonia**
Greece

*www.uom.gr*

**Ruprecht-Karls-Universität**
Heidelberg

*www.uni-heidelberg.de*

**SET University**
Ukraine

*www.setuniversity.tech*

**KVS**
Ukraine

*pkvfp.ki ev.ua*

**American Farm School**
Greece

*www.afs.edu. gr*

**ASCEND Consulting**
Malta

*ascendconsulting.eu*

**Ukrainian Academy of Cyber Security**
Ukraine
*https://uacs.kiev.ua/*

**REACH Innovation**
Austria

*www.reach-innovation.eu*

# Table of Contents

Co-funded by the European Union

## ABOUT THE PROJECT

The EnCycLEd Erasmus+ Project aims to promote digital readiness in cybersecurity, resilience, and capacity-building in educational institutions. To achieve this, the project will promote cybersecurity literacy and awareness. It focuses on training students, schoolteachers and other teaching professions to develop key digital skills and competences.

Special focus is given to promote interconnected educational systems in Europe with cybersecurity awareness and training at High Schools, Vocational Schools, as well as at university courses, especially the ones related to the formation of future teachers. The project results are planned to go beyond the project's educational partners, taking effect also via interactions with the vast existing network of associated institutions of the partners.

The EnCycLEd consortium benefits from the diverse and profound experience of higher education partners, professional schools and associations in the topic areas of cybersecurity and didactics. The project counts with cybersecurity expertise coming from European Universities (UIBK in Austria and HU in Germany) and from a cybersecurity association (UACS in Ukraine), supported by two other Universities (UoM in Greece and SET Univ. in Ukraine) to develop and test the training materials and school curricula. Two project partners (AC in Malta and REACH in Austria) will respectively cater for the development of the project's digital platform and the project’s dissemination and network-building. EnCycLEd will devote main efforts on interacting and piloting its developments in cooperation with two European Schools (in Greece and in Austria) and with two Ukrainian educational institutions (a University dedicated to the formation of teachers and a Vocational School).

## INTRODUCTION

The EnCycLEd pilot helps schools test five age-appropriate modules (for ages 10–14 and 15–18) that strengthen students' cybersecurity awareness, safety and digital resilience. At the same time, it gives teachers ready-to-use lessons and a light, practical way to evaluate what works. The pilot also supports Erasmus+ priorities on digital transformation and key competences.

This **Piloting Program Guide** (Guide) is the ***coordination and reporting blueprint*** for EnCycLEd piloting. It explains who does what and when, defines the minimum piloting packages (Options A/B/C), sets out the National Piloting Calendar approach, and describes how Key Performance Indicators (K1–K7 and D1–D7) are collected and reported to WP4 using the MEL Toolkit (Annexes E1–E8) EnCycLEd_WP4_MEL. Detailed classroom activities and lesson examples are contained in the separate **Program Development** document EnCyLEd_PROGRAM DEVELOPMENT, which teachers should use alongside this Guide.

# Section 1 - Program Overview And Prerequisites

## 1.1 Piloting Objectives and Expected Outcomes

The EnCycLEd platform (**https://go.encycled.eu**) is an open digital learning environment designed to promote cybersecurity awareness, digital literacy and responsible online behaviour among students aged 10–18. This Piloting Program Guide supports schools, school leaders and national partners in organising and monitoring the pilot, while teachers use the Program Development document for day-to-day lesson delivery.

### Objectives

During the piloting phase, participating schools are expected to:

- enable learners to grasp core notions such as **threats, passwords, privacy, social engineering, resilience, defence and cyberpeace**, and to name at least one concrete habit they will change in their online behaviour;
- support teachers to confidently run engaging, age-appropriate **5×45-minute lessons**, using the EnCycLEd **Modules, Resources, Glossary and Guides**, and to log brief reflections plus mini-quiz results;
- ensure that each school returns a short summary report outlining learning highlights, technical notes and improvement suggestions.

### Expected Outcomes

By the end of the pilot:

- **Students** will demonstrate improved understanding of cyber threats, password management, social media safety and data privacy, and will be able to describe safer digital habits.

- **Teachers** will be able to plan and deliver interactive 45-minute lessons using the EnCycLEd modules and resources, and to integrate light assessment (quizzes, reflections) into their practice.
- **Schools** will provide a short feedback report summarising learning outcomes, student engagement, technical challenges and suggestions for the next iteration of the materials and platform.

**Connection to EU Digital Education Priorities**

The piloting aligns with key European policy frameworks, including:

- the **Digital Education Action Plan (2021–2027)**;
- the **DigComp 2.2 Framework for Citizens**, particularly competence area 4 "Safety";
- the **Council Recommendation on Key Competences for Lifelong Learning (2018)** – Digital Competence; and
- the **ENISA Cybersecurity Skills Framework**, by introducing foundational awareness of cybersecurity roles.

**Prerequisites**

To participate effectively in the EnCycLEd piloting, schools should meet the following basic conditions:

- **Target group:** students aged 10–14 and 15–18; teachers of Informatics, Digital Literacy or related subjects.
- **Lesson duration:** 45 minutes per session (lessons can be combined into 90-minute blocks for projects).
- **Technical setup:** internet access, computers/tablets (approx. 1 device per 1–2 students), projector or interactive board.

- **Teacher preparation:** basic understanding of internet safety and ability to navigate online learning platforms.

- **Language:** English or localised versions of materials (e.g. Ukrainian, Greek, Maltese, etc.), according to national planning.

**Minimum piloting package per school (Options A, B, C)**

To ensure that piloting is both realistic for schools and sufficient to meet the project KPIs, each piloting institution is expected to implement **at least one minimum piloting package**. As a rule, piloting schools should implement either:

- **Option A – Full package**: all five modules, at least one career-guidance activity using the Guides, and multiple uses of the Discussions section with around **50–60 students**; or

- **Option B – Core package**: at least three modules (**Module 1, one technical module and Module 5**), plus at least one Guides activity, and at least **two purposeful Discussions activities** with **30–40 students**.

In exceptional cases, and only with prior agreement from **WP4 (UACS)**, a school may implement a lighter **Option C** (at least one module, one Guides activity and one use of Discussions with **20–30 students**), provided that this does not compromise the overall minimum targets in the KPI annex (students reached, modules delivered, cross-country activities and platform use).

Whichever option they choose, all piloting schools still contribute to the main project KPIs (modules delivered, cyber hygiene and resilience, and career awareness) and offer at least one structured activity on cybersecurity careers and study routes. National partners may encourage some schools to go beyond the minimum package (e.g. deliver all five modules plus multiple careers activities), but every piloting school must implement at least Option A, Option B or Option C for its participation to count towards the EnCycLEd piloting KPIs.

The detailed numeric minima per school and partner, including platform registration and outreach targets, are summarised in **Annex B – Piloting Schools KPIs** and **Annex D – Minimum Piloting Package and Piloting-related KPIs per Partner**.

## 1.2 Alignment with Project KPIs and Deliverables

### Purpose

This section explains how school-level activities in the EnCycLEd pilot link to the project's Key Performance Indicators (KPIs) and Deliverables (D4.1–D4.6) in Work Package 4 (Piloting and Evaluation). In other words, it shows how what you do in school turns into measurable project results.

### A. Relation Between Classroom Activities and Project Deliverables

Each activity conducted in the pilot phase generates practical evidence that contributes to the achievement of specific deliverables. The table below summarises the correspondence between school-level actions, deliverables, and KPIs.

| School-Level Activity | Linked Deliverable | Expected Output/ Evidence | KPI Contribution | Responsible Actor |
|---|---|---|---|---|
| **Teacher onboarding and access check** | D4.1 / D4.2 | Attendance record, readiness checklist | 100–150 teachers trained | National partner / School |
| **Delivery of EnCycLEd modules (1–5)** | D4.3 | Lesson logs, student worksheets, screenshots | ~1,000 students reached; ≥80 % module completion | Teacher / School |
| **Application of EnCycLEd materials and glossary** | D4.1 / D4.2 | List of used resources, localised materials | ≥100 digital resources used or adapted | School / WP2 |

| | | | | |
|---|---|---|---|---|
| **Cross-learning sessions with partner schools** | D4.5 | Short report, screenshots, shared board | ≥5 international exchanges conducted | WP4 / Schools |
| **Assessment and reflection (Pre/Post quiz)** | D4.4 | Aggregated quiz results, student reflections | +30 % knowledge improvement; ≥75 % post-quiz accuracy | Teacher / Evaluator |
| **Submission of final summary and feedback** | D4.3 / D4.6 | One-page report, highlights of lessons learned | 4 national summaries; 5 dissemination events | National partner / Consortium |

*Table 1: Correspondences between school-level actions, deliverables, and KPIs.*

## B. Deliverable–KPI Alignment Matrix

| Deliverable | Deliverable Title | Main KPIs Tracked | Evidence Sources |
|---|---|---|---|
| **D4.1** | Piloting Framework and Methodological Guide | Guide finalised and distributed; training sessions completed | Final guide, training records |
| **D4.2** | Teacher Training Materials | Five modules localised and uploaded to platform | Training toolkit, slide decks |
| **D4.3** | Piloting Implementation Reports | Four national reports; 1,000 students reached | Teacher logs, school reports |
| **D4.4** | Evaluation and Impact Report | ≥30 % learning improvement; ≥75 % post-quiz success rate | Quiz data, reflection forms |
| **D4.5** | Cross-Learning Casebook | At least five international lessons or exchanges | Activity reports, screenshots |
| **D4.6** | Policy and Practice Recommendations | Policy briefs and final dissemination results | National reports, event summaries |

*Table 2: Deliverable–KPI Alignment Matrix.*

## C. Monitoring and Reporting Flow

Data collected throughout the pilot follows a clear four-level reporting pathway:

**Teacher → School Summary → National Partner → EnCycLEd Consortium**

1. Individual lesson results, quiz outcomes, and observations are recorded at classroom level.
2. Schools compile one summary report aggregating their local results.
3. National partners consolidate reports from participating schools into a Country Implementation Report (D4.3).
4. The consortium aggregates data from all countries for the Evaluation Report (D4.4) and Cross-Learning Casebook (D4.5).

All data remain anonymous and compliant with GDPR and Erasmus+ ethical standards.

## D. KPI Measurement Timeline

| Stage of Pilot | Timeframe | Measured Indicators | Linked Deliverables |
|---|---|---|---|
| **Preparation** | Weeks 1–2 | Number of teachers trained; baseline readiness | D4.1 / D4.2 |
| **Implementation** | Weeks 3–10 | Number of modules delivered; student engagement | D4.3 |
| **Mid-point Reflection** | Week 8 | Student motivation; accessibility; inclusion | D4.3 |
| **Final Evaluation** | Weeks 11–12 | Quiz improvement; participation rate | D4.4 |

| | | | |
|---|---|---|---|
| **Cross-Learning Phase** | Months 24–30 | Number of joint lessons; cooperation quality | D4.5 |
| **Dissemination Phase** | Months 30–36 | Stakeholder participation; visibility | D4.6 |

*Table 3: KPI Measurement Timeline.*

## E. Optional (Extended) Indicators

Beyond the contractual KPIs, the pilot allows monitoring of additional indicators that enhance project visibility and sustainability.

| Extended Indicator | Purpose | Measurement Tool |
|---|---|---|
| **Student-produced content (videos, posters, campaigns)** | Demonstrates creativity and communication skills | Uploaded artefacts / photos |
| **Parental involvement activities** | Strengthens school–home cooperation in cyber hygiene | Parent feedback form |
| **Teacher peer mentoring and exchange** | Builds professional community and sustainability | Reflection log |
| **Use of bilingual resources** | Promotes inclusivity and accessibility | Lesson checklist |

*Table 4: Extended Indicators.*

These indicators are optional but recommended for schools wishing to document broader educational impact.

## F. Expected Contribution to Project Evaluation

All data gathered through the alignment process will feed directly into:

- **D4.3** – national implementation summaries;

- **D4.4** – overall impact and learning evaluation;
- **D4.5** – cross-learning and best-practice documentation;
- **D4.6** – final policy recommendations and sustainability planning.

## G. KPI dictionary

### *K1–K7 (piloting & participation)*

- **K1** – Teachers and students directly involved in piloting (teachers who taught at least one EnCycLEd module + students who took part in the piloted lessons).
- **K2** – Teachers (and future teachers) registered on go.encycled.eu (with platform accounts).
- **K3** – Students registered on go.encycled.eu (with platform accounts).
- **K4** – Other teachers / future teachers informed about the platform (beyond those directly piloting).
- **K5** – Students informed about the platform (e.g. assemblies, school events, campaigns, non-piloting classes).
- **K6** – Cross-country teams (teachers or students) formed and interacting on the platform.
- **K7** – Cross-country learning and exchange sessions (e.g. joint lessons or Discussion-based activities).

### D1–D7 (Discussions & cross-learning)

- **D1** – Teachers who used Discussions (created or joined at least one Discussion Group).
- **D2** – Discussion Groups created (class-level and cross-country groups).

- **D3** – Cross-country Discussion Groups (with participants from at least two countries).
- **D4** – Students in Discussion Groups (students with access to at least one Discussion Group).
- **D5** – Guest cybersecurity professionals / role models who took part in Discussions or Q&A linked to the platform.
- **D6** – Interactions in Discussions (posts and replies; approximate total).
- **D7** – Qualitative description of types of exchanges in Discussions (reflection, Q&A, group work / teamwork, cross-country debate, etc.).

**H. Piloting Timeline and Completion Deadline**

All piloting activities must fit within the EnCycLEd project timeline. In practice, this means that teaching, data collection and reporting at school and country level have to finish early enough to allow cross-country evaluation and final reporting.

• **By 30 June 2026** – piloting schools submit their school-level piloting reports and KPI data, including short descriptions of any cross-country activities.

• **By 15 July 2026** – piloting partners compile National Piloting Synthesis Reports and national KPI dashboards.

• **By 31 July 2026** – the platform team provides consolidated platform and Discussions usage statistics, and all piloting results are in the hands of WP4 (UACS).

This staging allows the Cross-Country Evaluation & Sustainability Assessment (Task 4.6) to take place between 31 July and 15 October 2026 in line with the project Gantt chart, and ensures that all contracted KPIs can be reported before the final project end date (**30 November 2026**).

## 1.3 Roles of partners during piloting

1. **Piloting schools (AFS, SU, KVS)**

a. Deliver the chosen **piloting package (Options A/B/C)** in classrooms (modules + Guides + Discussions).

b. Register and inform the agreed minimum numbers of **students and teachers** on / about the Platform.

c. Implement **cross-country and Discussions-based activities**, and complete the **school-level piloting reports and KPI forms**.

2. **HEIs (UIBK, HU, UoM)**

   a. Pilot EnCycLEd modules and resources with their own **students and/or future teachers**, where relevant.

   b. Register and inform the minimum numbers of **students and other teachers** specified in the KPI annex.

   c. Contribute to **cross-country teams and learning activities** and support analysis of piloting results with subject-matter expertise.

3. **UACS (WP4 Leader – Implementation, Piloting, Evaluation, Sustainability)**

   a. Leads **Work Package 4**, including design of the **Piloting Program** and **Piloting Guide**.

   b. Defines and maintains the **piloting KPIs, minimum targets and MEL templates**, and sets **internal reporting deadlines**.

   c. Aggregates school and country data, runs the **Cross-Country Evaluation & Sustainability Assessment (Task 4.6)**, and prepares lessons-learned outputs.

4. **AC (platform & training – WP3)**

a. Develops and maintains the **EnCycLEd Platform** and supports teachers and partners in using **Modules, Resources, Guides, Links and Discussions**.

b. Provides **technical support** for cross-country learning and exchange sessions on the platform.

c. Supplies **platform usage statistics** (registrations, Discussion Groups, interactions, etc.) needed for the piloting KPIs and MEL.

5. **REACH (dissemination & sustainability – WP5)**

a. Leads **dissemination, communication and sustainability** activities using evidence from piloting.

b. Ensures that **piloting results, cross-learning examples and KPIs** are visible in project events, materials and policy messages.

Works with UACS and other partners to connect piloting evidence to **sustainability and exploitation plans.**

# SECTION 2 - ONBOARDING AND ACCESS

## 2.1 Access to go.encycled.eu and encycled.eu

During the piloting phase, schools will primarily use **go.encycled.eu** as their teaching and learning platform. The **encycled.eu** website provides additional information about the project, news items, and links to outputs, but is not required for everyday classroom use.

👉 https://go.encycled.eu

Teachers and school coordinators should familiarise themselves with the main menu of go.encycled.eu, where all educational content is organised into **six sections**:

- **Modules**
- **Resources**
- **Glossary**
- **Guides**
- **Links**
- **Discussions**

The platform is web-based and can be accessed via a standard browser on school computers, laptops or tablets. The preferred entry point for teachers during piloting is **go.encycled.eu**.

## 2.2 Accounts / Sign-In

The EnCycLEd platform follows a simple access model that distinguishes clearly between **open educational content** and **restricted collaborative spaces**:

**Open access (no sign-in required):** Modules, Resources, Glossary, Guides, Links

These sections can be viewed and used freely by teachers, students, and other interested users without creating an account.

**Restricted access (sign-in required):** Discussions

This section is only available to vetted educators and invited students within specific, teacher-managed groups.

To support safe and well-organised piloting, the following rules apply:

**Teacher accounts**

Teachers who will participate in piloting are first validated by the relevant EnCycLEd partner organisation (e.g. as part of the National Piloting Plan).

After validation, the platform administrator creates teacher accounts and sends login details to the teacher's official email address.

In case of technical issues with sign-in or access, teachers can contact the platform support team at the email address provided by the coordinator (AscendConsulting) or via the contact form indicated in the onboarding materials.

**Creating Discussion Groups and inviting students**

Once logged in, teachers can create Discussion Groups (e.g. for one class, for a cross-country exchange, or for a Q&A with a guest professional).

Teachers then add or invite students to specific groups, following their school's procedures and the national piloting plan (for example, only students from a given class or participating schools).

Teachers are responsible for moderating the activity in their groups and for ensuring that all posts follow the project's Behaviour and Safety Policy.

**Student accounts, parental consent, and legal compliance**

Where individual student accounts are used, schools must ensure that all national legal requirements are respected (including data protection and child-protection rules).

Parental/guardian consent must be obtained whenever required by national law, school policies, or local practice before students are given access to Discussion Groups.

Students should receive a simple, age-appropriate explanation of the rules for using the platform and the Discussions section.

This access and sign-in model ensures that teaching materials remain openly available, while collaborative online spaces are protected, moderated, and compliant with national and school-level requirements.

## 2.3 Steps for working with the Platform (Modules, Resources, Glossary, Guides, Links, Discussions)

In practice, a typical piloting teacher will:

1. **Explore Modules** – select which module(s) and lessons fit their curriculum and timeframe.
2. **Check Resources** – download or bookmark supporting activities, games, and worksheets.
3. **Use the Glossary** – integrate key terms into lesson plans, homework, or revision.
4. **Plan with Guides** – choose at least one careers/study pathways activity from the Guides section.
5. **Share Links** – point students to trusted external sites for further exploration.
6. **Activate Discussions** – create or join appropriate Discussion Groups to extend learning.

These steps should be embedded into the **school-level piloting plan** and reflected in the country's National Piloting Calendar (for example: weeks where a cross-country Discussion is planned, or a Q&A with a cybersecurity professional is organised).

**Discussions section – purpose and pedagogy**

The Discussions section is an integral part of the piloting concept and should be used in a purposeful, structured way. It is designed to support:

- Peer-to-peer learning within a class
  - short written reflections after a lesson (e.g. "one thing I learned / one question I still have");
  - small group follow-up on tasks started in class (e.g. developing a class cyber hygiene charter).
- Cross-country exchanges
  - joint discussion threads where students from different countries share perspectives on the same activity;
  - collaborative challenges (e.g. comparing cyber-safety posters, campaigns, or class rules).
- Interaction with guest cybersecurity professionals / role models
  - asynchronous Q&A, where students submit questions and receive written replies;
  - short "Ask a cyber-pro" sessions following a live or recorded talk.

Teachers should always:

- set clear rules and prompts for each Discussion;



Co-funded by the European Union

- moderate contributions in line with school and project behaviour and safety policies;
- ensure that no personal or identifying information is shared by students.

Planned use of Discussions – including any cross-country activities or sessions with guest professionals – should be scheduled in advance and reflected in the National Piloting Calendar so that it aligns with classroom lessons, avoids peak assessment periods, and contributes to the piloting KPIs on student engagement, collaboration and use of the platform.

## 2.4 Orientation Videos on the use of the Platform

Introductory videos and platform tutorials are available on the Homepage section of the Platform (https://go.encycled.eu/) and once a teacher has Sign-in to the Platform Discussions section. Also via the main EnCycLEd website (https://encycled.eu).

Teachers can use these materials before starting the pilot to:

- Understand the pedagogical structure of EnCycLEd.
- Learn how to combine modules and resources into lessons.
- Review examples of implementation in partner schools across Europe.

# SECTION 3 - IMPLEMENTATION ROADMAP (BLUEPRINT TIMELINE)

## 3.1 Phases: Plan → Prepare → Deliver → Review

The EnCycLEd piloting process follows a simple four-phase learning cycle (Plan → Prepare → Deliver → Review), based on widely used digital education frameworks (UNESCO ICT-CFT, DigCompEdu, Erasmus+ Digital Education Action Plan). It ensures that teachers can move smoothly from initial planning to implementation and reflection, while maintaining flexibility for different school contexts.

The four phases (Plan → Prepare → Deliver → Review) are further translated into the classroom learning phases (Phase 0–3). For detailed examples of how to apply these phases in lessons, please see *Program Development, Section 2.1.2 "The teaching material sequence".*

**Planning the minimum piloting package in each school**

When drawing up their National Piloting Calendar and school-level implementation plans, partners should ensure that each piloting school is clearly assigned to Option A (full), Option B (core) or Option C (flex) as defined in Section 1.1.

Schools following Option A should use the semester or academic-year plan to schedule all five modules, plus at least one career-guidance activity from the Guides section.

Schools following Option B should ensure that their plan includes, at a minimum: Module 1, one technical module (Module 2, 3 or 4), Module 5 (Cyberpeace), and one structured activity based on the Guides section (e.g. a 45-minute career lesson or similar).

Schools following Option C should plan at least one module (any module that fits their context) and one structured careers activity using the Guides.

In all cases, the selected modules and the Guides-based activity should be:

placed on specific calendar dates in the National Piloting Calendar (not just "Week 1–12" labels);

aligned with the overall EnCycLEd timeline so that all teaching, reflection and data collection finish well before 30 November 2026; and

clearly linked to the relevant KPIs in the logical framework (e.g. number of modules delivered per school, number of students reached, increase in cybersecurity awareness, and exposure to cybersecurity careers and study pathways).

This approach gives schools flexibility (through Options A, B and C) while ensuring that every piloting school makes a meaningful and measurable contribution to the project's agreed piloting and careers-related indicators.

| Phase | Duration | Core Actions | Outputs / Evidence |
|---|---|---|---|
| **1. PLAN** | 1–2 weeks | Teachers explore the EnCycLEd platform, identify which modules (1–5) fit their curriculum, and set a realistic schedule. They also check available digital resources (devices, internet connection) and decide whether lessons will be conducted in English or translated locally. | – Pilot timetable<br>– Selected modules (10–14 / 15–18)<br>– Brief note on technical readiness |
| **2. PREPARE** | 1 week | Teachers familiarise themselves with each module's materials (videos, games, worksheets) and the corresponding glossary terms. They adapt instructions for their age group, prepare printouts or slides if needed, and test links to games or videos in advance. | – Lesson plans / slide decks<br>– Printed or saved materials<br>– Checklist of tested resources |
| **3. DELIVER** | 4–6 weeks | Teachers conduct 45-minute lessons following the playbooks for Modules 1–5. Each session begins with a short warm-up question, proceeds through guided exploration and a practical activity | – Attendance list (optional)<br>– Screenshots of classroom activity or digital tasks |

| | | | |
|---|---|---|---|
| | | (e.g. game, quiz, group task), and ends with a reflection discussion. Teachers take short notes on timing, student engagement, and comprehension. | – Mini-quiz results<br>– Teacher reflection notes |
| **4. REVIEW** | 1 week | Teachers summarise the experience by collecting short student reflections ("What did I learn about staying safe online?") and compiling a brief school summary report. The report highlights what worked well, challenges encountered (e.g. connectivity, language barriers), and recommendations for improvement.<br>Post-Pilot Reflection Workshop: online session where all pilot teachers share key experiences, best practices, and propose improvements for next EnCycLEd cycle. | – One-page school summary report<br>– Samples of student work<br>– Lessons learned for next iteration (for example, 1 collective Miro board summarising lessons learned (evidence for D4.4 and D4.5)) |

*Table 5: Piloting phases.*

Planned use of the **Discussions** section (e.g. class reflections, cross-country exchanges, Q&A with experts) should be built into the school's timeline and National Piloting Calendar; see **Section 2 (Onboarding and Access)** for practical guidance on how to set up and manage Discussion Groups.

## 3.2 Semester / Academic-Year Calendar

The sample **12-week semester timeline** below is a **blueprint**, not a rigid prescription. It illustrates a balanced pacing of preparation, module delivery, reflection, and reporting over a school term.

In practice, **each national partner must translate this sequence into a National Piloting Calendar with concrete dates**, using:

- the shared EnCycLEd **Gantt / Excel timeline**; and
- their own **national school calendar** (start/end of term, holidays, exam periods, school events).

Partners may merge or stretch weeks (for example, combining activities from two "weeks" into one busy school week, or spreading one module over more time). However, when doing so they must still:

- ensure that all planned piloting activities and data collection are completed **no later than 30 November 2026**; and
- keep **1–2 months buffer** after the end of school-level piloting for national aggregation and final reporting.

The **National Piloting Calendar** is thus the main reference for checking whether local piloting fits within the EnCycLEd timeline and whether the deadlines for reports and deliverables are realistic.

| Week | Activity | Responsible |
|---|---|---|
| **1–2** | Teacher onboarding: exploring EnCycLEd platform, checking internet access and devices | Teacher |
| **3** | Lesson 1 – *Module 1: What is Cybersecurity?* | Teacher |
| **4–5** | Lesson 2 – *Module 2: Who was it?* | Teacher |
| **6–7** | Lesson 3 – *Module 3: What can we do against it?* | Teacher |
| **8** | Mid-point reflection: teacher notes on student engagement and lesson flow | Teacher |
| **9** | Lesson 4 – *Module 4: What is Cyber Defense?* | Teacher |
| **10** | Lesson 5 – *Module 5: Cyberpeace* | Teacher |
| **11** | Post-pilot quizzes and student reflection activity | Teacher |
| **12** | Preparing and submitting short pilot summary report | Teacher |

*Table 6: Piloting calendar.*

## 3.3 Milestones

| Milestone | Description | Evidence |
|---|---|---|
| **M1** | School registration for the pilot | Confirmation email / list of schools |
| **M2** | Teacher onboarding completed | Attendance sheet / feedback form |
| **M3** | All modules planned in the school's piloting package (Options A/B/C) delivered | Lesson logs / screenshots |
| **M4** | Feedback collected | Online form / short summary |
| **M5** | School report submitted to national coordinator | Final compiled document |

*Table 7: Milestones.*

To support this planning, an **EnCycLEd National Piloting Calendar Template** is provided in *Annex 2*. Each **piloting partner / educational institution** who delivers modules and classroom activities is requested to complete this template for their country, indicate the piloting schools involved, and share the finalised National Piloting Calendar with the project coordinator by the agreed deadline. It does not apply to partners whose role is primarily technical support, evaluation or coordination.

# SECTION 4 - SCHOOL ROLLOUT PLAN (BLUEPRINT RUNBOOK)

The School Rollout Plan provides a step-by-step guide for teachers to deliver the EnCycLEd piloting in a structured yet flexible way. It combines curriculum planning, age-appropriate pedagogy, light data collection, and practical technical management. All actions can be led by a single teacher – no additional coordinator is required.

## 4.1 Planning Academic Load and Calendar

### Pedagogical perspective

Children and teenagers learn best when cybersecurity is connected to their real experiences – online games, social media, or mobile devices. Therefore, the modules should be embedded naturally into existing lessons on digital literacy, computer science, civic education, or life skills. Avoid presenting cybersecurity as a "threat-only" topic; instead, frame it as empowerment – "how to be smart, safe, and confident online".

### Practical implementation

1. **Integrate, don't overload.**

Each module replaces or complements an existing ICT or safety lesson. Keep the same rhythm – one 45-minute lesson every two weeks.

2. **Build progression.**

    - Module 1: awareness and terminology (introduce key words).
    - Module 2: cause–effect thinking (incident analysis).
    - Module 3: problem-solving and resilience.
    - Module 4: systems thinking (defence strategies).

- Module 5: empathy and digital citizenship.

3. **Plan variety.**

Alternate formats – discussion, video, group challenge, creative task – to sustain attention spans (10–14 yrs ≈ 20 min; 15–18 yrs ≈ 30 min).

4. **Allow reflection time.**

Young learners need time to process feelings about online risks. Reserve 5 minutes at the end of each lesson for short journaling or pair discussion.

## 4.2 Teacher and Materials Preparation

Effective preparation goes beyond testing links. Teachers should anticipate misconceptions and prepare prompts that guide discovery. For example, when teaching about phishing, students may think "hackers always look scary"; prepare examples showing how messages can appear friendly.

| Step | Why it matters (pedagogical focus) | Practical tip |
|---|---|---|
| **Select age-appropriate materials** | Younger learners need concrete, visual examples; older ones prefer logic and autonomy. | Use comics for 10–14, discussion cases for 15–18. |
| **Localise language** | Helps inclusion and comprehension. | Translate only keywords on slides; keep English terms like "cybersecurity", "firewall" visible to build digital vocabulary. |
| **Prepare starter questions** | Activates prior knowledge and curiosity. | "Who protects your phone?", "Have you ever seen a fake message?" |
| **Create visual anchors** | Aids memory and focus. | Display 3 icons: 🧠 Think 🔒 Protect 💬 Share Safely. |

| | | |
|---|---|---|
| **Coordinate with parents** | Reinforces learning at home. | Share the sample parent letter and suggest 3 safety rules to discuss as a family. |

*Table 8: Preparation steps.*

**Inclusive practice**

● Encourage both girls and boys equally to lead tech-related tasks.

● Support students with limited digitalaccess by allowing pair-work or printed versions.

● Use simple, concrete language; explain one new term at a time.

## 4.3 Lesson Delivery and Minimal Data Collection

**Methodological guidance**

1. Warm-up (5 min) – Activate curiosity

Use an everyday scenario ("Your friend sends you a strange link—what do you do?"). Let students vote or raise hands.

This lowers anxiety and connects learning to real life.

2. Explore (10–15 min) – Present new knowledge

Keep explanations short (no more than 7 minutes of teacher talk). Alternate with visuals or questions every 2 minutes to keep attention.

3. Apply (15–20 min) – Learning by doing

Use teamwork or short simulations. Younger groups love role-play (pretend to be "cyber detectives"), while older ones prefer analysing case studies or playing strategy games like Cyber Crime Time.

4. Reflect (5–10 min) – Personal meaning

Ask: "What will I do differently online after this lesson?"

Students can write it on sticky notes, for example.

| What | Purpose | How to collect |
|---|---|---|
| **Pre-question** | Measure initial awareness | Ask orally, note 3–4 keywords |
| **Mini-quiz** | Reinforce facts | 3–5 short questions (paper or digital) |
| **Student reflection** | Capture attitude change | One sentence or emoji rating 🙂😐☹️ |
| **Teacher log** | Continuous improvement | 3 lines after class: what worked / what to change |

*Table 9: Evidence collection (light-touch).*

The goal is learning, not testing. The data help refine teaching, not grade students.

## 4.4 Technical Support (Platform Access and Troubleshooting)

### Methodological note

Teachers should present technical troubleshooting as a *learning opportunity*: show students that problem-solving is part of digital resilience. If the internet fails, explain calmly: "Technology isn't perfect – let's see how we can adapt." This models flexible thinking.

### Checklist before class

- Test Wi-Fi and open all platform pages in browser tabs.
- Prepare one offline backup (printed worksheet or screenshot).
- Check sound and projector brightness.
- Log in 10 minutes before students arrive.

| Issue | Pedagogical handling | Quick fix |
|---|---|---|

| | | |
|---|---|---|
| **Video doesn't load** | Turn it into a discussion: "Based on the title, what do you think the video shows?" | Reload page or summarise content verbally. |
| **Students distracted by screens** | Use the "eyes-on-teacher" signal (hand raise or short sound cue). | Pause and refocus with a mini-question. |
| **Mixed skill levels** | Pair confident students with those needing support. | Assign peer-mentor roles ("Tech Helper"). |
| **Limited devices** | Shift to team tasks using shared screens. | 3–4 students per device is fine for games or quizzes. |

*Table 10: Common classroom scenarios.*

The EnCycLEd rollout is not just about transferring knowledge – it is about shaping safe, responsible, and confident digital citizens. Teachers act as facilitators, guiding curiosity, dialogue, and reflection. By combining structure (modules, quizzes) with empathy and creativity, every classroom – regardless of size, language, or resources – can successfully pilot the five EnCycLEd modules and make cybersecurity a natural, engaging part of everyday learning.

# SECTION 5 - MODULES – PLAYBOOKS

The EnCycLEd Modules are the core learning units of the platform. Each module offers ready-to-use classroom content designed for two age groups (10–14 and 15–18) and is structured into clear learning phases that help teachers deliver engaging, age-appropriate lessons on cybersecurity.

## 5.1 General Guidance for Working with Modules

### Module page structure

Each module page on go.EnCycLEd .eu contains:

- A short introductory description of the theme.
- Separate versions for two age groups.
- Embedded multimedia materials (videos, worksheets, comics, or games).
- A list of learning objectives and discussion prompts.
- Links to relevant items from the Resources, Glossary, and Guides sections.

Each module follows a simple but powerful 4-phase learning framework, aligned with inquiry-based and experiential learning. Each phase should take 5–15 minutes within a 45-minute lesson.

| Phase | Focus | Teacher role | Student activity |
|---|---|---|---|
| **Phase 0 – Introduce** | Capture attention and connect to daily life | Facilitate a short discussion or show a short video | Share prior experiences or opinions |
| **Phase 1 – Explore** | Build understanding through examples | Present key concepts and vocabulary | Identify cyber risks, explain in own words |

| | | | |
|---|---|---|---|
| **Phase 2 – Apply** | Practise and test understanding | Guide activity, game, or mini-case | Solve problems, make decisions |
| **Phase 3 – Reflect** | Consolidate learning and attitudes | Ask reflective questions, summarise main points | Express "What I learned / will do differently" |

*Table 11: Pedagogical phases.*

### Inclusive methodology

- Use visual examples for 10–14 group (cartoons, icons, emojis).
- Encourage discussion and reasoning for 15–18 group.
- Alternate individual + teamwork to include both introverted and active students.
- Reinforce with positive feedback: focus on safe choices, not mistakes.

### Using Discussions with the modules

During piloting, teachers are encouraged to use the **Discussions** section to reinforce and extend the work started in class. For example:

- After each **module or lesson**, teachers can open a short **reflection thread** where students post 1–2 sentences on what they found most interesting, surprising or challenging.
- For **Module 5 (Cyberpeace)**, a cross-country Discussion Room can host a structured debate on a guiding question (e.g. *"How can we contribute to cyberpeace in our school and community?"*). Students from different countries compare experiences and comment on each other's ideas.
- For any module, a teacher can invite a **guest cybersecurity professional** (nationally or from another partner country) to respond to students' questions in a dedicated Q&A thread.

When preparing their **National Piloting Calendar**, teachers and national coordinators should schedule these online activities so that they take place **within**

**1–2 weeks of the relevant lessons**, and so that they feed into the **Review / reflection** phase of each module. The mapping between the four operational phases (Plan → Prepare → Deliver → Review), the learning phases (Phase 0–3).

## 5.2 Module 1 – *What is Cybersecurity?*

### Access (URL)

👉https://go.EnCycLEd.eu/modules/what-is-cyber-security/

Available in two versions:

- **For 10–14 years old** – simplified definitions and visual examples.
- **For 15–18 years old** – deeper reflection and open-ended tasks.

| Category | Examples / Content | How to use |
|---|---|---|
| **Video** | "Introduction: What is Cybersecurity?" (animated short) | Play at the beginning of the lesson to spark curiosity. |
| **Worksheet** | "My Digital Footprint" | Print or share digitally; students mark safe/unsafe behaviours. |
| **Infographic** | "5 Golden Rules of Online Safety" | Use to summarise the lesson visually. |
| **Glossary terms** | Cybersecurity, Malware, Password, Phishing, Personal data, Digital footprint | Explain 2–3 per lesson; ask students to give real examples. |
| **Additional resources** | Short comic from Resources Repository; ENISA "Cyber Safety Tips for Students" | Optional homework or group reading. |

*Table 12: Core Materials / Resources / Literature / Glossary.*

## Pedagogical rationale

This first module introduces the *language and logic* of cybersecurity. It helps students realise that cybersecurity is not abstract – it touches everyday actions like password creation, app installation, and social media sharing.

| Domain | Name of Domain | Comments |
|---|---|---|
| **Learning Outcomes** | Acquire the basic principles of cyber security<br>Strengthen teamworking skills<br>Improve understand of core principles | |
| **Teaching method** | Individual study<br>Interactive<br>Group work<br>Educational game | |
| **Learning Setting /Activity Description** | Preparation:<br>- Read through narrative of module 1.<br>- Print the list of questions of core concepts<br>- You will need to divide the class into similar groups depending on overall size, e.g. five students in five groups)<br>Option A (Home assignment)<br>- Pose two questions for home work:<br>1) How could Irina have done better (solved her problems more effectively and more efficiently) or worse (i.e. exacerbating her situation)?<br>2) If you had been in Irina's situation, to whom had you turned for help, when and why?<br>Option B (Class assignment)<br>- Put two assignments to the five groups à five students:<br>1) Each group prepares two things in 20 min:<br>a) 3 students answer the following question: How could Irina have done better (solved her problems more effectively and more efficiently) or worse (i.e. exacerbating her situation)? By drawing up a list of suggestions of better/worse;<br>b) the other 2 students prepare a list of core concepts and principles in the narrative.<br>2) You pose questions in turn to each group for answers to assignment 1 and you count the number of plausible answers by each group on the white board.<br>Announce a score at half time to raise expectations!<br>Then turn to the core concepts mentioned in the text: each group shall explain one concept of its choosing to the class; you evaluate the quality of the explanation and give between 1-3 points; you ask, at least, each group to explain one core concept. You may, in addition, use the | |

| | | |
|---|---|---|
| | quiz cards to test the general understanding of cyber security terms in the class.<br>Finally, you nominate a winning group, highlighting the respective skills in answering questions/assignments. | |
| **Evaluation/Reflection** | At the end of the class, the participants are encouraged to self-reflect and evaluate how they answered the questions | In comparison to traditional (analog) weapons, 'cyber weapons' regularly require collusion of the victim. In this case Irina enabled the attack first by a weak password and second being attracted by a social phishing campaign.<br>Cyber weapons have less permanent, i.e. reversible effects, they disrupt but rarely destroy and thus can be used preferably for signaling/extortion. In addition, cyber weapons may have many targets but may perish in scale effect soon (cf. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2421554/differentiating-kinetic-and-cyber-weapons-to-improve-integrated-combat/) |
| **Supporting materials (online)** | Questions for home assignment<br>List of core concepts and brief descriptions<br>Presentation with quiz slides<br>(Additional audios/videos) | |
| **Material for Parents** | Letter for parents | |

*Table 13: Teacher Feature of Module 1.*

For a more detailed introduction to the material and preparation for classes, another version of the lessons is also available, in accordance with phases 0-3.

| Phase | Time | Teacher actions | Student tasks | Learning outcome |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **Phase 0 – Introduce** | 5 min | Ask: "How many apps did you use today?" or "What could happen if someone accessed your phone?" | Students answer freely; list common risks on board. | Awareness of personal connection to cybersecurity. |
| **Phase 1 – Explore** | 10–15 min | Play the video "What is Cybersecurity?" and discuss examples of safe vs unsafe online behaviour. Present 2–3 glossary terms. | Listen, take notes, share personal examples. | Understand core concepts: threats, protection, data safety. |
| **Phase 2 – Apply** | 15–20 min | Hand out the worksheet "My Digital Footprint". Ask students to mark which actions are safe, risky, or need checking. For older group, discuss "What information would you never post online and why?". | Work individually or in pairs; compare answers. | Can identify unsafe digital habits and propose improvements. |
| **Phase 3 – Reflect** | 5–10 min | Ask: "Which of the five Golden Rules will you follow starting today?" or "How could you teach this to a younger student?" | Share 1–2 sentences orally or on sticky notes. | Internalise responsible digital behaviour and peer awareness. |

*Table 14: Lesson Flow (Phase 0–3).*

### Differentiation

- For **10–14 group**, use more visuals and limit abstract vocabulary.
- For **15–18 group**, extend discussion with examples of global cyber incidents or media stories.
- Encourage peer mentors (older students) to help younger ones explain concepts.

### Assessment

**Goal:** Measure understanding, not memorisation. Keep the process short and formative.

### Success indicators

- Students can define cybersecurity in their own words.
- Students identify at least **three safe online practices**.

- Students demonstrate curiosity and readiness to apply what they learned at home.

| Tool | Purpose | Example questions / prompts |
|---|---|---|
| **Mini-quiz (5 questions)** | Check comprehension of key terms. | 1. What does cybersecurity mean?2. Give one example of a strong password.3. What is a digital footprint?4. Why should we not share our location online?5. What is phishing? |
| **Student reflection card** | Assess self-awareness and attitude change. | "One thing I will do differently online is…" |
| **Teacher observation** | Track engagement and misconceptions. | Use a quick checklist: Participation ✓ / Needs support ✓ / Excellent understanding ✓ |
| **Peer activity (optional)** | Promote collaboration. | Students design a poster "How to stay safe online". |

*Table 15: Assessment.*

**Teacher's tip:** "Start this first module with enthusiasm and humour. When students see cybersecurity as something connected to their lives – not as rules or fear – they open up. Always end with an empowering message: *'You are the first defender of your digital world.'*"

## 5.3 Module 2 – *Who was it?* (Network Security)

### Access (URL)

👉https://go.EnCycLEd.eu/modules/module-2-this-is-a-test/

Two versions: **10–14** and **15–18**.

| Type | Example Content | Purpose in Class |
|---|---|---|
| **Interactive Story** | "Who was it?" – a mystery of a hacked school computer | Introduce students to cyber-incident investigation |
| **Worksheet** | "Identify the Suspect!" | Practise reasoning and teamwork |



Co-funded by the European Union

| | | |
|---|---|---|
| **Comic strip (optional)** | "Digital Detectives" (from Resources Repository) | Visual reinforcement for 10–14 group |
| **Glossary terms** | Hacking, Phishing, Social Engineering, Identity Theft | Explain key attack types and behavioural signs |

*Table 16: Core Materials / Resources / Glossary.*

This module answers the question: when does the public disclosure of a cyber attack, through attribution, is problematic and for whom?

| Domain | Name of Domain | Comments |
|---|---|---|
| **Learning Outcomes** | Acquire basic knowledge of reacting to a cyber incident<br>Improve understanding of core problems in incident reaction<br>Strengthen teamworking & research skills | Depending on the administrative structure of your state, cyber incident responses require multilevel & multi-entity collaboration |
| **Teaching method** | Individual study<br>Interactive<br>Group work<br>Presentation; Q & A | The module combines a fictional story line (based on the cyber attack on the German municipality Bitterfeld) with a student assignment to research "real cases of cyber incident responses" |
| **Learning Setting /Activity Description** | Preparation:<br>- Read through story of module 2.<br>- Print the list of key concepts (Glossary)<br>1. Familiarize yourself with the underlying core problem of the disclosure dilemma.<br><br>Home assignment<br>2. Assign the reading of the comic and ask to identify the four main plot lines of the story: Lena & Juan (Friends); the Municipality (Institutions and their interests); the experts; the federal state level (international considerations)<br>- You will need to divide the class into similar groups along the four plot lines (depending on overall size, e.g. five students in four groups)<br><br>Class assignment<br>- Pose two questions to each of the groups:<br>1) When and why could any person/institution in your plot line have concealed information from another person/institution? (15 min. | Which institutions/persons are present in your municipality/federal state to prevent, address or follow-up care in cases of cyber security breaches? |

| | | |
|---|---|---|
| | discussion in group with consensual answer to be presented in class).<br>2) Research five "real cases" on the internet in which a municipality has been attacked via cyber space and explain to the class (later on) how the persons, institutions in your plot line have been affected (25 min.)<br>Each group prepares two answers for a 10 min presentation:<br>- Has there been a strong incentive to conceal information about a malicious incident among persons/institutions in your plot line, if so, why so? (2 min of pro and con)<br>- Which of the real cases did you choose and why? What astonished you most about these cases?<br>Finally, you reflect upon what you, as a teacher, learned from the students, highlighting the respective skills in answering questions/assignments. | |
| **Evaluation/Reflection** | At the end of the class, the participants are encouraged to self-reflect and evaluate how they answered the questions | Contextualizing the Module:<br>Malicious cyber incidents often trigger "disclosure dilemmas" (cf. Harnisch et al., 2020), these disclosure dilemmas arise when a person/institution possess private information whose public dissemination would yield some benefits (incrimination of the perpetrator) but would also trigger considerable costs, e.g. social stigma or reputational losses after acting carelessly.<br><br>Harnisch, Sebastian / Zettl, Kerstin/Hansel, Mischa (2022): Einleitung: Asymmetrien und Cyberkonflikte, in (Eds.): Asymmetrien in Cyberkonflikten. Wie Attribution und der Einsatz von Proxies die Normentwicklung beeinflussen. Wiesbaden: Nomos, 19-29<br><br>Toth, K. E., Yvon, F., Villotti, P., Lecomte, T., Lachance, J. P., Kirsh, B., … Corbière, M. (2021). Disclosure dilemmas: how people with a mental health condition perceive and manage disclosure at work. Disability and Rehabilitation, 44(25), 7791–7801. https://doi.org/10.1080/09638288.2021.1998667<br><br>Carnegie, A. and Carson, A. (2019), The Disclosure Dilemma: Nuclear Intelligence and International |

| | | |
|---|---|---|
| | | Organizations. American Journal of Political Science, 63: 269-285. https://doi.org/10.1111/ajps.12426<br><br>2. In comparison to traditional (analog) weapons, 'cyber weapons' regularly require collusion of the victim. In this case a vulnerability in the firewall enabled the hackers to gain access to the systems of the IT provider of the municipality and the whole city administration got paralyzed.<br>Cyber weapons have less permanent, i.e. reversible effects, they disrupt but rarely destroy and thus can be used preferably for signaling or like in this case for extortion. In addition, cyber weapons may have many targets but may perish in scale effect soon (cf. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2421554/differentiating-kinetic-and-cyber-weapons-to-improve-integrated-combat/) |
| **Supporting materials (online)** | List of key concepts (Glossary)<br>List of worksheets (1 for home assignment, 1 for class assignment)<br>Supplementary literature (list + copies)<br>(Additional online resources) | |
| **Material for Parents** | Letter for parents | |

*Table 17: Teacher Feature of Module 2.*

For a more detailed introduction to the material and preparation for classes, another version of the lessons is also available, in accordance with phases 0-3.

| Phase | Time | Teacher actions | Student tasks | Learning outcome |
|---|---|---|---|---|
| **Phase 0 – Introduce** | 5 min | Pose a hook question: "Have you ever heard of a computer being hacked?" | Share stories or opinions | Interest activated; connect to real world events |
| **Phase 1 – Explore** | 10 min | Read or show the intro of Who was it? | Identify characters and possible motives | Understand how cyber incidents begin |

| | | | | |
|---|---|---|---|---|
| **Phase 2 – Apply** | 20 min | Guide the group through digital clues (e-mails, passwords, USB, etc.) | Work in teams to find the culprit and justify decision | Practise critical thinking and digital forensics |
| **Phase 3 – Reflect** | 10 min | Lead debrief: "What mistakes allowed the attack?" | Propose prevention measures | Recognise the importance of good cyber hygiene |

*Table 18: Lesson Flow (Phase 0–3).*

### Differentiation

- 10–14 yrs → act out roles of suspect/victim/investigator.
- 15–18 yrs → analyse log entries or timeline diagram.

### Assessment

| Tool | Purpose | Example questions / prompts |
|---|---|---|
| **Short quiz (4 Qs)** | Recall key ideas | "What is social engineering?" / "Name one sign of phishing." |
| **Group presentation** | Collaboration | Explain your investigation in 2 minutes. |
| **Reflection sentence** | Metacognition | "How can I avoid being tricked online?" |

*Table 19: Assessment.*

### Success indicators

Students can explain how social engineering works and identify at least two ways to protect themselves.

## 5.4 Module 3 – *What can we do against it?* (Cyber Resilience)

### Key Activities

- **Game:** *Cyber Crime Time* (official ENISA educational game)
- **Final Quiz:** summary of Modules 1–3



Co-funded by the European Union

## Access (URL)

👉https://go.encycled.eu/modules/module-3-what-can-we-do-against-it/

| Type | Example Content | Purpose in Class |
|---|---|---|
| **Game** | Cyber Crime Time (simulates attacker decisions) | Students learn by reverse thinking – what makes systems vulnerable |
| **Worksheet** | Build Your Cyber Shield | Plan preventive steps for school network or devices |
| **Infographic** | "How to Recover After a Cyber Incident" | Discuss resilience and recovery |
| **Glossary** | Resilience, Backup, Firewall, Incident Response | Anchor new terms during debrief |

*Table 20: Core Materials / Resources / Glossary.*

This module answers the question: what are cyber threats, how are they conducted and how to protect oneself in cyber space?

| Domain | Name of Domain | Comments |
|---|---|---|
| **Learning Outcomes** | Acquisition of basic knowledge of attack techniques and patterns of cyber attacks<br>Acquisition of the ability to identify common attack vectors such as phishing, social engineering or malware and the ability to protect yourself from cyber-attacks by using strong passwords, detecting phishing or the usage of VPNs<br>Strengthen teamworking, group discussions, student's self-efficacy, critical evaluation<br>[Optional: Gain basic knowledge of how to use digital translation software] | The module combines a game about cybersecurity (Cyber Crime Time) with a classroom debate about the rights and the responsibility of students in cyber space. Within this debate pupil will explore the dilemma between their own responsibility, freedom, risk and security, regulations and band? (cf. prevention paradox: If the effectiveness of cybersecurity is marked by the absence of visible incidents, how do Cyber security/IT teams prove the need for continuous measures and funding?) |
| **Teaching method** | Individual study<br>Interactive<br>Group work<br>Quiz Presentation; Q & A | |
| **Learning Setting /Activity Description** | Preparation:<br>- Read through the story on the homework worksheet about the undercover white hat hacker and print it out for your class<br>- have a look at the Online Game "Cyber Crime Time" (or the translated version | 1. In comparison to traditional (analog) weapons, 'cyber weapons' regularly require collusion of the victim. In this case the hacker gained access to the secret recipe of SLURP by phishing and vishing. Cyber weapons have |

| | | |
|---|---|---|
| | (PDF), if required also print or share the Game translation with your students<br>- Print the list of key concepts (Glossary)<br><br>Home assignment<br>- Assign the reading of the white hat hacker story and playing the online game Cyber Crime Time as homework (the link to the game is provided on the homework worksheet)<br>Class assignment<br>- You may test the gained knowledge of your students first by using the quiz to test the general understanding of the key take aways of the game and answer general questions of the students<br>- Divide the class into four groups (with approx. 5 persons per group) for an in-class debate about the following question: "Should the school regulate the general media use and the online behavior of pupils or not?"<br>Group 1: Argues for the regulation of the online behavior; they should choose 2 main discussants<br>Group 2: Argues against the regulation of the online behavior; they should choose 2 main discussants<br>Group 3: Jury, they will evaluate the discussion and the arguments and will select the winners (they count the arguments quantitatively, they will evaluate them qualitatively and they will also evaluate the interaction behavior (do they react to the arguments of the opposite or not?)<br>Group 4: General audience, they will judge the Jury in the end<br>- the whole debate will approx. take 30 minutes, but the students will need some time for preparation (ca. 15 minutes)<br>- after the preparation time, the two debating groups will start with an opening statement (2 minutes per person) and then an exchange of words follows (approx. 12 minutes)<br>- the jury and the audience listen, take notes and evaluate<br>- after the exchange of words, the closing statement follows (1 minute person)<br>- the jury and the audience will then have a brief amount of time to discuss | less permanent, i.e. reversible effects, they disrupt but rarely destroy and thus can be used preferably for signaling or like in this case for extortion. In addition, cyber weapons may have many targets but may perish in scale effect soon (cf. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2421554/differentiating-kinetic-and-cyber-weapons-to-improve-integrated-combat/)<br>2. The prevention paradox describes the situation in which successful prevention measures can lead to the problem they were intended to combat becoming barely visible - which paradoxically leads to the necessity of prevention being called into question such as compulsory seatbelts or mass immunizations (cf. Thompson 2016). This concept can also be applied within cyberspace. When effective preventive measures are in place, cyberspace may appear to be safe, leading individuals and organizations to become less careful. This false sense of security can result in careless behavior, such as using weak passwords, ignoring security updates, or underestimating the risk of phishing attacks. As a consequence, new vulnerabilities emerge, ultimately enabling cyber threats to resurface and exploit these weaknesses.<br><br>Thompson, C. (2018), Rose's Prevention Paradox. J Appl Philos, 35: 242-256. https://doi.org/10.1111/japp.12177<br>For German speakers: https://leitbegriffe.bzga.de/alphabetisches-verzeichnis/praeventionsparadox/ |

| | | |
|---|---|---|
| | their evaluation (max. 5 minutes) and will choose the winner of the debate<br>Finally, if you still have some time left you reflect within class what the students learned from the online game and the debate and discuss questions | |
| **Evaluation/Reflection** | At the end of the class, the participants have basic knowledge of how to protect themselves against cyber-attacks and they are encouraged to self-reflect and evaluate to their personal responsibility in cyber space | |
| **Supporting materials (online)** | List of key concepts (Glossary)<br>Homework Worksheet<br>Supplementary literature (list + copies)<br>(Additional online resources) | |
| **Material for Parents** | Letter for parents | |

*Table 21: Teacher Feature of Module 3.*

For a more detailed introduction to the material and preparation for classes, another version of the lessons is also available, in accordance with phases 0-3.

| Phase | Time | Teacher actions | Student tasks | Learning outcome |
|---|---|---|---|---|
| **Phase 0 – Introduce** | 5 min | Ask: "What would you do if your device was infected with a virus?" | Brainstorm reactions | Recognise need for preparedness |
| **Phase 1 – Explore** | 10 min | Explain concept of resilience and show infographic | Take notes of preventive actions | Understand protection measures |
| **Phase 2 – Apply** | 20 min | Play Cyber Crime Time (game) in pairs; pause after each decision to analyse consequences | Decide, reflect, compare results | Grasp how choices affect security |
| **Phase 3 – Reflect** | 10 min | Guide discussion: "What makes a person or organisation cyber-resilient?" | Summarise 5 protective habits | Adopt personal resilience strategies |

*Table 22: Lesson Flow (Phase 0–3).*

## Assessment

| Tool | Purpose | Example questions / prompts |
|---|---|---|
| **Final Quiz (8 Qs)** | Evaluate knowledge from Modules 1–3 ("Cyber Basics Review") | 1. List two ways to prevent phishing. 2. Why are backups important? |
| **Group Poster** | Encourage creativity | Create a poster "5 Steps to Cyber Resilience". |
| **Teacher observation** | Monitor teamwork and problem-solving | Checklist of participation and reasoning. |

*Table 23: Assessment.*

### Success indicators

Students articulate preventive measures and demonstrate understanding that cybersecurity = continuous practice, not a one-time action.

## 5.5 Module 4 – *What is Cyber Defense?*

### Access (URL)

👉 https://go.EnCycLEd.eu/modules/what-is-cyber-defense/ *(to be added officially to the platform)*

Recommended for ages **15–18** or advanced students 10–14.

| Type | Example Content | Purpose in Class |
|---|---|---|
| **Video** | Inside a Security Operations Centre (SOC) | Demonstrate real-world defensive roles |
| **Article** | "Understanding Cyber Defense Layers" | Base text for group reading and summary |
| **Worksheet** | "Design a Defense Plan for Our School Lab" | Collaborative strategy exercise |
| **Glossary** | Firewall, Network Defense, SOC, Incident Detection, Ethical Hacker | Key vocabulary for discussion |

*Table 24: Core Materials / Resources / Glossary.*

This module answers the question: what are the layers of cyber defense, and how do components like incident detection and ethical hacking contribute to overall security?

| Domain | Name of Domain | Comments |
|---|---|---|
| **Goals** | Goal 1: Education! Students understand key concepts and topics related to cyber defence.<br>Goal 2: Creativity! Students process information into journalistic texts and learn how to present information to others in a comprehensible and creative way. | |
| **Learning Outcomes** | Students can critically analyse interviews with experts and extract relevant information. They prepare individually and then discuss their results in a group. This promotes cooperation and the ability to compromise. | |
| **Learning Setting /Activity Description** | Students can critically analyse interviews with experts and extract relevant information. They prepare individually and then discuss their results in a group. This promotes cooperation and the ability to compromise. | |
| **Teaching materials** | introductory PowerPoint-presentation "Module 4: Cyber Defender" | Lessons can be started with a menti survey. A survey can be created under this link and a QR code can be inserted into the corresponding slide |
| **Student materials** | → glossary<br>→ work sheets<br>→ interview videos<br>→ interview transcripts | Please ensure students can access the online video interviews and watch them themselves (via headphones and separate devices). Alternatively, feel free to adjust the lesson structure and assign the videos as homework |
| **Material for Parents** | parental letter | |

*Table 25: Teacher Feature of Module 4.*

For a more detailed introduction to the material and preparation for classes, another version of the lessons is also available, in accordance with phases 0-3.

| Phase | Time | Teacher actions | Student tasks | Learning outcome |
|---|---|---|---|---|
| **Phase 0 – Introduce** | 5 min | Ask: "Who protects the internet?" Show photo of cyber defenders at work. | Predict their jobs and tools. | Interest in career roles. |

| | | | | |
|---|---|---|---|---|
| **Phase 1 – Explore** | 10 min | Play SOC video and explain multi-layer defense concept. | Take notes on tools and teams. | Understand organizational defense structures. |
| **Phase 2 – Apply** | 20 min | Facilitate team task to create a defense plan for school computer lab. | Map risks, decide controls, draw diagram. | Apply systems thinking to security. |
| **Phase 3 – Reflect** | 10 min | Debrief: "What makes a good cyber defender besides technical skills?" | Share ideas (e.g., teamwork, responsibility). | Link defense skills to citizenship values. |

*Table 26: Lesson Flow (Phase 0–3).*

### Assessment

| Tool | Purpose | Example questions / prompts |
|---|---|---|
| **Peer review** | Evaluate group plans | "Which part of this plan is most realistic?" |
| **Reflection form** | Encourage career thinking | "Would you like to work in cyber defense and why?" |
| **Teacher notes** | Monitor concept grasp | Checklist of risk identification accuracy. |

*Table 27: Assessment.*

### Success indicators

Students demonstrate basic understanding of defense strategies and recognise cyber defense as a collaborative, ethical effort.

## 5.6 Module 5 – *Cyberpeace*

### Guiding Questions

- What does peace mean in digital spaces?
- How can we prevent conflict and hate online?
- What is my responsibility as a digital citizen?

### Access (URL)

👉https://go.encycled.eu/modules/module-5-cyberpeace/

| Type | Content | Usage |
|---|---|---|
| **Video** | "Words That Build, Not Break" | Set emotional tone for lesson |
| **Worksheet** | "Kindness Challenge Checklist" | Students track positive online actions for a week |
| **Creative Task** | Digital poster or short video campaign for cyberpeace | Culminating activity |
| **Glossary** | Cyberbullying, Digital Footprint, Online Etiquette, Empathy, Respect | Vocabulary for discussion |

*Table 28: Core Materials / Resources / Glossary.*

This module answers the question: what is cyberpeace and what kind of cyber-peaceful world do we want to live in together?

| Domain | Name of Domain | Comments |
|---|---|---|
| **Goals** | **Goal 1: Positivity!** Concluding the project with an overall more positive and future oriented focus, building up upon module one to four.<br>**Goal 2: Skill building!** Promoting simulation-skills (self-reflection, self-efficacy, organisation and efficacy in a social group) among the students.<br>**Goal 3: Vision of a cyber-peaceful world!** Creating a vision of the cyber-peaceful world the students want to live in. | |
| **Learning Outcomes** | The lesson is divided into 3 levels:<br>Level 1: the individual: self-reflection (creating distance between one's own opinion and the role position taken in the simulation)<br>Level 2: the group: self-efficacy (ability to initiate processes within a group: initiator role)<br>Level 3: the structure: efficacy in a wider social context (ability to convince, to find compromises and make consensual decisions: role: leader) | You will also find the skills in the simulation structure so that you know which skills are trained in which part of the lesson. |
| **Learning Setting /Activity Description** | After an introduction delivered by the teacher, the students will simulate a fictional Dynamic Coalition of the Internet Governance Forum (IGF), aiming at formulating principles of a cyber-peaceful world. | |

| | | |
|---|---|---|
| **Teaching materials** | → Introductory PowerPoint-presentation "Introducing the topic cyberpeace"<br>→ teacher feature 1 "structure and goals"<br>→ teacher feature 2 "literature review"<br>→ additional material<br>→ printable role cards | Lessons can be started with a menti survey. A survey can be created under this link and a QR code can be inserted into the corresponding slide. |
| **Student materials** | → students' material 1 "role script"<br>→ students' material 2 "fact sheet 'Internet Governance Forum (IGF)'"<br>→ students' material 3 "rolesheet chairperson"<br>→ glossary | More role scripts are provided than may be required. This is to ensure that the module is suitable for classes of different sizes. |
| **Materials for parents** | → Parental letter (Why do the students carry out a simulation about cyberpeace?) | |

*Table 29: Teacher Feature of Module 5.*

## Proposed Structure of the Lesson

Disclaimer: This is a proposed teaching structure for a typical 90-(2x45)-minutes-lesson, that of course can be adjusted to how the teacher wants to structure his lesson.

| | description | skills | materials | duration |
|---|---|---|---|---|
| **Preparation** | The students should read their role sheets carefully and prepare their positions, arguments and an opening statement in their groups. At the same time, the speaker and correspondent of each group should be determined. | • self-reflection<br>• self-efficacy in a group<br>• organizing a group | role scripts | at home |
| **Part 1: Introducing the topic "cyberpeace"** | An introduction into the topic "cyberpeace" is delivered by the teacher, bringing everyone up to the same level and finding out what prior knowledge the students have. The PowerPoint-presentation prepared by the EnCycLEd-team can be used for this part. | connecting prior and new knowledge | Teacher material "literature review" Power-Point-presenta-tion | 15 minutes |
| **Part 2:** | The Internet Governance Forum (IGF), a multistakeholder-group will be simulated by groups of | • self-reflection<br>• self-efficacy<br>• efficacy in a social group | simulation structure role scripts | 60 minutes |

| | | | | |
|---|---|---|---|---|
| **Simulating the IGF** | students that embody a specific role. The goal is to discuss how cyberpeace can be achieved and to agree on a final report that would be ready to be submitted to decision-makers for consultation. | organizing a group | fact sheet "Internet Governance Forum (IGF)" glossary | |
| **Part 3:**<br><br>**Recapitulating the lesson** | Finally, the students will recapitulate their learning outcomes. They are expected to name what they will take out of this lesson. There should also be room for commenting on what worked well in die simulation and where the students faced difficulties. | 1. evaluating a group process<br>recapitulating and fostering learnings | - | 15 minutes |

*Table 30: Proposed Structure of the Lesson.*

**Simulation Structure**

In this module, the process will take centre stage (how can we achieve cyberpeace effectively?) to develop skills related to simulations.

**Simulated conference**:

The Internet Governance Forum (IGF) is a multistakeholder-group aiming at dialogue concerning several issues of Internet governance. The students will simulate on of the Dynamic Coalitions (DC) that are dedicated to a specific governance issue. For this simulation, a hypothetical new DC, the "**Dynamic Coalition on Cyberpeace**" is created. They are required to submit an DC session report to the annual IGF, summarizing the discussions and containing the output, they collectively produced. (detailed information on the DCs can be read here)

**Leading question:**

What measures are necessary to build and maintain a peaceful and secure cyberspace for everyone?

**Groups**:

Groups of four to five students are to be formed. Each group embodies/ plays all together one of the following roles:

- **technical sector**: > a head of a large technology company (e.g. Microsoft)
- **private sector:** > a CEO of a cybersecurity company (e.g. CrowdStrike)

> a head of a Social Media platform (e.g. Meta)

- **civil sector:** > a teenager who uses Social Media frequently > a NGO director (e.g. Cyberpeace Institute, Human Rights Watch)
- **political sector:** > a representative of a government of a liberal state (e.g. Germany) > a representative of a government of an illiberal state (e.g. China)
- **academic sector:** > an university expert

Note: *If a class is too small the group size can be reduced. In addition, the numbers in front of the sectors can be used as a guide to prioritize them. For smaller classes, the aim should be for each sector to be represented once*.

One student in each group is to be chosen as correspondent who represents the group in (informal) debates with the other groups.

Apart from the groups, a head of the meeting must be nominated. His/ her tasks include ensuring that the rules of the discussion are observed and moderating the discussion. He is also responsible for writing down the points that have been agreed upon in order to present them at the end. The teacher should introduce this person briefly to the chairperson role (*see document "rolesheet_chairperson"*).

| round | timing | description | procedural notes | trained skills |
|---|---|---|---|---|
| **Homework:** Read the simulation carefully. Work your way through the scripts and find together in your group. Discuss in your group what your opening statement should look like and what points you want to make in the discussion in order to get them into the IGF meetings report. You can use the positions listed under point 2 as a guide and develop arguments on | | | | self-reflection<br>self-efficacy in a group<br>organizing a group |



Co-funded by the European Union

| | | | | |
|---|---|---|---|---|
| this basis. Agree on one correspondent (who may speak in informal talks with other groups to coordinate statements) and one speaker (who publicly represents the group in the formal meeting and delivers the opening statement).<br>Apart from the groups, a head of the meeting must be nominated. His/ her tasks include ensuring that the rules of the discussion are observed and moderating the discussion. He is also responsible for writing down the points that have been agreed upon in order to present them at the end. | | | | |
| **1 – group preparation** | 5 minutes | Meet up in your group, prepare briefly and get on the same page. | | |
| **2 – public meeting** | 1-2 minutes per group (in total: 10 minutes) | Three-minute briefing of the president on the issue to be discussed.<br>Opening statements by one person per group. | The head of the meeting (e.g. president) will recognize the participants in the order in which they request to speak, and no participant may speak again if others have not yet spoken. | self-efficacy in a group |
| **3 – informal meeting** | 45 minutes | Debate each participant's proposed points.<br>Edit, add, or drop proposed points and combine them into a report. | The head of the meeting (e.g. president) will recognize participants in the order in which they request to speak. Participants should limit their statements to one to three minutes each. Each participant can request a three to five-minutes break during which the participants can move around freely and negotiate on their points. individually or in small groups. | willingness to compromise<br><br>efficacy in a wider social context (in this part, diplomatic space is provided so that students learn to experience each other's positions in order to find the win set and compromise with the lowest common denominator)<br><br>persuasion<br><br>Setting processes in motion |
| **4 – public meeting** | 10 minutes | Hear the draft report.<br>Agree on a final report that fully reflects the discussions and which is ready to be submitted to | | willingness to compromise<br><br>efficacy in a wider social context |

| | | | | |
|---|---|---|---|---|
| | | decision-makers for consultation. | | |

*Table 31: Lesson's simulation.*

Note: *The structure of the simulation is based on the educational materials of the Council of foreign relations. Additional information can be found under this link.*

Please also note that the in-class simulation is primarily designed for students aged 14–18. If you are teaching a younger age group (e.g. 10–14) but would still like to work with this module, you could instead focus on introducing the concept of Cyber Peace and discussing it together in class in a more informal way, without carrying out the full simulation.

Another option would be to use the discussion rooms on the EnCycLEd platform for a virtual simulation. In this case, you can create a discussion room named "Dynamic Coalition on Cyberpeace" and assign each group a home task to publish one short entry (a few sentences) reflecting their group's position in the discussion room. Students should also familiarise themselves with the positions/entries of other groups and write any relevant comments or questions they may have. Afterwards, you can review the group positions together in class, address the comments and questions, and emphasise that cyber peace should take into account the perspectives and interests of all relevant stakeholders.

Of course, you may also choose to conduct the in-class simulation itself if you feel your students are ready for it – you know your class best and can decide which approach works best for them.

**Success indicators**

Students use respectful language, show empathy, and propose collective actions for a safer, kinder digital environment.

**Methodologist's Note for All Modules**

• Alternate short bursts of information with activity every 10–12 minutes.

• Keep "visible learning" tools – board posters, term cards, emojis.



Co-funded by the European Union

- Encourage peer teaching (older students mentoring younger ones).
- End each lesson with one positive action students can apply immediately online.

# SECTION 6 - RESOURCES REPOSITORY – OPERATIONAL USE

The EnCycLEd Resources Repository is a central library of curated digital learning materials that support and enrich the five core modules. It allows teachers to select age-appropriate multimedia content to create engaging, flexible, and interactive cybersecurity lessons.

The repository contains more than 100 resources, all openly accessible, verified for educational use, and aligned with European standards for safe digital education.

## 6.1 Purpose and Resource Types

### Purpose

● To provide teachers with ready-to-use supplementary materials (for classroom or homework).

● To enable diverse learning formats – reading, listening, playing, discussing, reflecting.

● To promote digital literacy and critical thinking through authentic examples.

● To encourage cross-curricular use, connecting cybersecurity with civic education, ethics, and ICT.

| Type | Description | Recommended Use in Lesson | Example Title (on Platform) |
|---|---|---|---|
| **Article** | Short informative texts explaining cybersecurity concepts or case stories. | Reading comprehension, summarising activity, homework. | "Top 5 Ways to Protect Your Password" |
| **Comics** | Illustrated narratives simplifying complex ideas. | Intro for younger learners; visual storytelling. | "The Adventures of Cyber Cat and Phish" |
| **Game** | Interactive simulations or quizzes promoting experiential learning. | Main activity (Phase 2 – Apply). | "Cyber Crime Time", "Google Interland" |

| | | | |
|---|---|---|---|
| **Literature / Book Extracts** | Age-appropriate excerpts linking fiction to digital ethics. | Reading circle; discussion of moral dilemmas. | "The Digital Detective" |
| **Podcast** | Short audio pieces with experts or stories. | Listening exercise; reflection or note-taking task. | "Teens Talk Cyber" |
| **Presentation** | Slide decks summarising core ideas. | Visual support for explanation or recap. | "5 Rules of Online Safety" |
| **Quiz** | Pre- or post-lesson self-tests. | Assessment or energiser. | "Cyber Smart Challenge" |
| **Video** | Animated explainers or interviews. | Attention-grabber or content illustration. | "What Is Cybersecurity? " |
| **Worksheet** | Printable or digital templates guiding activities. | Individual or group work (Phase 2). | "My Digital Footprint", "Identify the Suspect" |

*Table 32: Resource Types and Typical Use.*

## 6.2 Parameters

Every resource is tagged with parameters to help teachers filter and select the right material quickly.

| Parameter | Meaning | Practical Advice for Teachers |
|---|---|---|
| **Applicability** | Which module(s) it supports (M1–M5). | Use filters like Module 1 or Module 5 to match lesson plan. |
| **Target Age** | Intended learner group (10–14 / 15–18). | Choose younger version for visual simplicity, older for deeper analysis. |
| **Language** | Original EN; some resources available in DE/EL/MT/UA. | Enable browser translation for local language. |
| **Theme** | Key topic area (e.g., Passwords, Phishing, Resilience, Cyberpeace). | Align theme with your current module focus. |
| **Learning Method** | Reading / Listening / Playing / Discussion. | Mix 2 methods per lesson (max) to keep focus. |
| **Format Length** | Short (<5 min) / Medium (5–10 min) / Long (>10 min). | For 45-min lessons choose 1 medium + 1 short item. |

*Table 33: Parameters.*

**Tip:** Always preview a resource at least one day before class to test loading speed, subtitles, and sound level. For younger learners, limit videos to 3–4 minutes; attention peaks decline after 7 minutes.

## 6.3 Patterns for Selecting Materials for a 45-Minute Lesson

A well-balanced 45-minute cybersecurity lesson ideally combines one core material, one activity, and one reflective or visual element. Below are three tested patterns.

| Phase | Activity | Resource Type | Timing |
|---|---|---|---|
| **0 – Introduce** | Ask warm-up question + show short video | Video (2–3 min) | 5 min |
| **1 – Explore** | Read comic or infographic in pairs | Comic / Infographic | 10 min |
| **2 – Apply** | Complete simple worksheet or quiz | Worksheet / Quiz | 20 min |
| **3 – Reflect** | Share learning and draw one "cyber rule" | Poster / Whiteboard | 10 min |

*Table 34: Pattern A – "Watch – Discuss – Do" (ages 10–14).*

| Phase | Activity | Resource Type | Timing |
|---|---|---|---|
| **0 – Introduce** | Brief discussion on real news article | Article | 5 min |
| **1 – Explore** | Play interactive simulation | Game (e.g., Cyber Crime Time) | 20 min |
| **2 – Apply** | Debrief with mini-presentation | Presentation / Discussion | 10 min |
| **3 – Reflect** | Answer 3 quiz questions + reflection sentence | Quiz / Worksheet | 10 min |

*Table 35: Pattern B – "Read – Play – Reflect" (ages 15–18).*

| Phase | Activity | Resource Type | Timing |
|---|---|---|---|
| **0 – Introduce** | Listen to a podcast extract | Podcast | 5 min |
| **1 – Explore** | Analyse message and keywords | Worksheet | 10 min |
| **2 – Apply** | Design a poster or social-media message | Creative Task | 20 min |
| **3 – Reflect** | Class presentation | Discussion | 10 min |

*Table 36: Pattern C – "Listen – Think – Create" (mixed ages).*

### Pedagogical recommendations

- Alternate **sensory modes** (listening, reading, acting) to reach all learners.

● End every lesson with a visual or tangible artefact (post-it rule, drawing, pledge) – it reinforces memory.

● For inclusion, allow verbal instead of written reflections.

● Use digital games sparingly (max once per 2 weeks) to preserve novelty and ensure discussion.

## 6.4 Integration with the Module Playbooks

Each module's playbook already lists two or three matching resources. Teachers can extend or adapt using the repository.

| Module | Core Theme | Suggested Extra Resources from Repository | Integration Tip |
|---|---|---|---|
| **M1 – What is Cybersecurity?** | Basics of safety and digital footprint | Video "Strong Passwords 101"; Comic "Cyber Cat Finds a Virus" | Use for warm-up discussion or homework assignment. |
| **M2 – Who was it?** | Incident investigation | Worksheet "Trace the Phish"; Podcast "Digital Detective Diaries" | Play podcast intro as scene setter. |
| **M3 – What can we do against it?** | Resilience and defence | Infographic "Backups Save the Day"; Game "Stop the Attack!" | Use infographic for post-game analysis. |
| **M4 – What is Cyber Defense?** | Network protection strategies | Video "Inside a SOC"; Presentation "Layers of Defense" | Combine with team planning worksheet. |
| **M5 – Cyberpeace** | Digital ethics and empathy | Article "Building Respect Online"; Poster Toolkit "Words That Build" | Use for creative campaign activity. |

*Table 37: Repository for teachers.*

Where relevant, teachers are encouraged to extend these module activities into the Discussions section (for example, by opening a class or cross-country thread for follow-up reflection); see Section 2 for details on using Discussions pedagogically during piloting.

# SECTION 7 - GLOSSARY – PRACTICAL USE

The **EnCycLEd Glossary** is an interactive digital dictionary that explains key cybersecurity and digital-safety concepts in clear, age-appropriate language. It is designed as both a teaching aid and a student reference tool, supporting comprehension and vocabulary development across all modules. More than 40 terms are available and continuously updated to align with current cybersecurity vocabulary.

## 7.1 Navigation

### Accessing the Glossary

Teachers and students can reach the glossary via the top menu on the EnCycLEd platform:

👉 **go.EnCycLEd.eu → Glossary**

Each entry contains:

- **Term** – the key word (e.g. *Phishing*).
- **Definition** – simple explanation adapted for non-experts.
- **"Read More" link** – extended description, examples, or related resources.
- **Related Modules** – tags showing where the term appears (e.g. *M1, M2*).
- **Cross-reference** – other glossary terms connected by topic.

### Using the Alphabet Index and Search

- Click any letter (A–Z) to browse alphabetically.
- Use the search bar to type keywords or partial words (e.g. "passw" → *password*, *passphrase*).

• The "Read more" button expands the definition to include a short paragraph and optional video or infographic.

**Pedagogical approach**

• Encourage students to explore the glossary independently before lessons ("Find 3 new terms and bring 1 example of each").

• Reinforce the idea that cybersecurity has its own language – knowing words builds confidence.

• For classes with younger students, read definitions aloud together, then match them with pictures or emojis.

## 7.2 Embedding Terms in Lesson Plans and Homework

### A. In Lesson Plans

Integrating glossary terms into every module helps students gradually build a shared "digital safety vocabulary". Each lesson should introduce 2–3 new terms and reuse previously learned ones for reinforcement.

| Phase | Teacher Action | Example (10–14) | Example (15–18) |
|---|---|---|---|
| **Phase 0 – Introduce** | Write or display 1–2 keywords on board. Ask: "Have you heard this word before?" | Password, Virus | Malware, Phishing |
| **Phase 1 – Explore** | Show the glossary definition. Let students restate it in their own words. | "So a virus is like a germ for computers." | "Phishing is when someone tries to trick you into sharing data." |
| **Phase 2 – Apply** | Use terms in group tasks or quizzes. | Match words → pictures. | Fill-in-the-blank sentences. |
| **Phase 3 – Reflect** | Ask students to connect term to their life. | "How can I avoid phishing?" | "Why does digital footprint matter for jobs?" |

*Table 38: Example of lesson plan.*

## B. In Homework and Projects

### Vocabulary Reflection Card

Ask students to choose three new terms they learned in a module and complete the table:

| Term | Definition (in own words) | Example from my life | Emoji that fits the word |
|---|---|---|---|
| **Phishing** | Tricking someone to give personal data | Fake email from "bank" | 🎣 |
| **Firewall** | Tool that blocks dangerous connections | School Wi-Fi protection | 🔥 |
| **Backup** | Copy of data kept safe | Photos in Google Drive | 💾 |

*Table 39: Sample homework task.*

### Extended Project (for older students 15–18)

- Assign short essays or posters "*Ten Cyber Words Every Citizen Should Know*".
- Require inclusion of glossary definitions and real-life examples.
- Let students present and explain one term to peers → peer teaching enhances confidence.

| Module | Core Concepts to Reinforce | Suggested Glossary Terms |
|---|---|---|
| **M1 – What is Cybersecurity?** | Basic safety language | Cybersecurity, Password, Phishing, Personal Data |
| **M2 – Who was it?** | Incident investigation | Hacking, Social Engineering, Identity Theft |
| **M3 – What can we do against it?** | Protection and resilience | Resilience, Backup, Incident Response |
| **M4 – What is Cyber Defense?** | Network protection roles | Firewall, Network Defense, SOC, Ethical Hacker |

| | | |
|---|---|---|
| **M5 – Cyberpeace** | Digital ethics and empathy | Cyberbullying, Digital Footprint, Online Etiquette, Respect |

*Table 40: Integrating Glossary Across Modules.*

## C. Methodological Advice

● Revisit older terms at the start of each lesson as a "Warm-up Glossary Quiz."

● Create a classroom "Word Wall" or digital Padlet with new terms and examples.

● Encourage students to draw icons for each term – visual memory aids comprehension.

● For mixed-ability groups, provide definitions in both English and Ukrainian side by side.

## D. Outcome

By systematically embedding glossary terms into lessons, students progress from passive awareness to active command of cybersecurity vocabulary, enabling them to talk confidently about online safety and ethical digital behaviour in both English and their native language.

# SECTION 8 - GUIDES – PRACTICAL USE

The EnCycLEd Guides are not just about careers – they are tools for shaping digital self-awareness, personal responsibility, and inspiration. For children and teenagers, understanding cybersecurity careers begins with understanding who they are online and how their daily habits connect to real professions that protect the digital world.

These guides help students move from *"I use technology"* → *"I understand how it works"* → *"I can protect it – maybe even as my job one day."*

## Guides as a required part of piloting and KPIs

During piloting, every participating school is expected to organise **at least one** structured activity using the Cybersecurity Careers and Study Pathways Guide. Use of the Guide counts towards the project **KPIs** on promoting cybersecurity studies and careers (see logical framework), and at least one such activity is expected in each piloting school. These activities provide concrete **evidence** for the indicators linked to WP2 (quality and relevance of guidance materials) and WP4 (impact of piloting on students' understanding of cybersecurity careers and study options).

Simple **examples** that schools can choose from or adapt include:

*"Find Your Cyber Match"* – students work individually or in pairs with the Guide to identify one or two roles that fit their interests and strengths, then post a short reflection (e.g. in the Discussions section or on paper) explaining why this role appeals to them and what skills they would need to develop.

*Career pathways mapping* – groups use the Guide to trace one concrete study pathway (e.g. from lower secondary to a specific vocational or university route) and create a short poster or slide explaining the steps, key decisions, and supporting subjects.

These activities should be scheduled in the **National Piloting Calendars** (e.g. as a 45-minute lesson or short sequence of two lessons) and reported in

school/national reports so they can be counted towards the agreed KPIs on career guidance, exposure to cybersecurity professions, and informed study choices.

## 8.1 Section Structure (Careers and Study Pathways)

### A. Educational Purpose

The Cybersecurity Careers and Study Pathways Guide is designed to bridge cyber hygiene education and career orientation. They show how small daily habits (using strong passwords, verifying information, respecting others online) are the same foundations that professionals rely on in cyber defence, risk management, policy, and digital ethics.

Each Guide section introduces:

- Digital Awareness – why cybersecurity matters for everyone, not only for "IT people".
- Cyber Roles and Pathways – examples of jobs in cybersecurity and the people behind them.
- Skills and Mindsets – curiosity, teamwork, ethical responsibility, resilience and other transferable skills.
- Education Pathways – how school subjects, VET routes and further study build the foundation for future expertise.
- Real-Life Stories – short, relatable examples of cybersecurity professionals from different backgrounds.

**Remember** to record Guides-based activities in your school report, as they feed into the career-awareness KPIs.

Careers and study pathways activities can also be supported through the Discussions section (e.g. "Ask a cyber-professional" threads or peer exchanges about future

plans). For instructions on creating and moderating such spaces, please refer to Section 2.

### B. How to Navigate and Use the Guides

Each Guide can be found under the "Guides" tab on go.EnCycLEd.eu. They are structured for use by teachers, school counsellors, and parents, and can be explored:

- in short classroom sessions (e.g. 30–45 minutes),
- as part of project days or STEM events, or
- through independent study and reflection.

| Section in Guide | Purpose for Students | How Teachers Can Apply It |
|---|---|---|
| **Career Snapshot** | Introduces the role (e.g., "Threat Hunter") | Use for storytelling or warm-up discussion. |
| **Skill Map** | Lists both hard and soft skills | Ask students to identify which they already have. |
| **Study Pathways** | Connects school subjects to professions | Build "My Learning Roadmap" posters. |
| **Real Voices** | Features quotes from real cyber experts | Inspire with diversity and human stories. |
| **Action Plan** | Small steps for today and future | Create mini-goals: "My 3 steps to stay cyber smart." |

*Table 41: Typical elements and how they can be used.*

### C. Pedagogical Logic Behind the Guides

As a teacher, remember that children relate best to people, not professions.

Introduce cyber careers through *human stories, curiosity, and purpose*, not through job titles alone. Instead of saying "You could be a penetration tester," say *"Some people help others by testing systems for weaknesses – like digital doctors who find health problems before they get serious."*

This approach:

- builds values first – empathy, responsibility, curiosity, fairness;

- then connects those values to skills and professions;
- and only then invites students to consider specific career options

## 8.2 Career-Orientation Lessons and Activities Using Guides

The Guides are most effective when used interactively, not as static reading. Each activity below follows the experiential cycle used in cyber hygiene training: *Notice → Explore → Apply → Reflect.*

| Element | Description |
|---|---|
| **Goal** | Students explore cybersecurity career profiles and identify the roles matching their strengths, interests, and values. |
| **Duration** | 45 minutes |
| **Methodological Focus** | Self-reflection, linking personality traits to professions, building self-confidence and ownership of learning. |
| **Resources** | EnCycLEd Career Guide – section "Roles in Cybersecurity" and Skill Map Worksheet. |
| **Lesson Flow (Steps)** | **1. Warm-up (5 min):** Ask "What's one thing online you'd like to make safer?" to engage emotional connection. **2. Explore (10 min):** Students browse 3–4 roles (e.g., SOC Analyst, Penetration Tester, GRC Officer, Awareness Trainer). **3. Apply (20 min):** Each student completes the Skill Map Worksheet, marking ✓ where they feel strong (communication, logic, creativity, leadership). **4. Reflect (10 min):** Round discussion – "Which cyber role suits who I am?" |
| **Expected Outcome** | Students identify 1–2 roles that resonate with their strengths and values (e.g., "I like solving puzzles → Threat Analyst"). |
| **Teacher Tips** | Emphasise that cybersecurity needs many types of minds – analytical, creative, empathetic. Reinforce positive feedback: "Your curiosity or communication skill is also a cyber skill." |

*Table 42: Activity 1 – "Find Your Cyber Match" (ages 15–18).*

| Element | Description |
|---|---|
| **Goal** | Help younger students see how everyday school subjects connect to digital professions and cyber hygiene. |
| **Duration** | 40 minutes |
| **Methodological Focus** | Linking academic learning to real-world application; building intrinsic motivation and digital curiosity. |

| | |
|---|---|
| **Resources** | EnCycLEd Guide – "Learning Roadmap"; paper sheets or digital templates for drawing. |
| **Lesson Flow (Steps)** | **1. Warm-up (5 min):** Ask: "Which school subjects help you use technology safely?" **2. Explore (10 min):** Teacher shows how subjects connect to cyber skills (Math → logic, Languages → communication, Art → design). **3. Apply (15 min):** Students draw a "My Path to the Future" map linking subjects to imagined careers (e.g., Art → UX Designer). **4. Reflect (10 min):** Share drawings and discuss which subjects they'll value more now. |
| **Expected Outcome** | Students see relevance of school learning to technology and safety; improved motivation. |
| **Teacher Tips** | Keep it playful and encouraging – focus on imagination, not precision. Praise effort and curiosity. Use stickers or icons (💻 🎨 🔍) to visualise skills. |

*Table 43: Activity 2 – "Cyber Pathway Map" (ages 10–14).*

| Element | Description |
|---|---|
| **Goal** | Promote inclusivity and show that anyone, regardless of gender, can succeed in cybersecurity. |
| **Duration** | 45 minutes |
| **Methodological Focus** | Challenging stereotypes, empathy building, respect for diversity in technology. |
| **Resources** | EnCycLEd "Women in Cybersecurity" stories and videos; printable quotes or role cards. |
| **Lesson Flow (Steps)** | **1. Warm-up (5 min):** Ask: "Who do you imagine when you hear 'cyber expert'?" List answers on board. **2. Explore (10 min):** Watch or read 2–3 real stories of women and men in cybersecurity. **3. Apply (20 min):** Groups create "My Digital Hero" posters with name, role, and contribution (real or fictional). **4. Reflect (10 min):** Class discussion – "How can we support equality in technology?" |
| **Expected Outcome** | Students recognise diverse role models and develop inclusive attitudes. |
| **Teacher Tips** | Use balanced examples of both men and women. Encourage students to choose heroes who inspire them personally (not just famous ones). Reinforce respect and teamwork as universal values. |

*Table 44: Activity 3 – "Women and Men Protecting the Internet" (mixed ages).*

| Element | Description |
|---|---|
| **Goal** | Transform cyber hygiene knowledge into collective responsibility and positive digital behaviour. |
| **Duration** | Two sessions × 45 minutes |
| **Methodological Focus** | From awareness to action – students co-create digital rules and take ownership of online safety. |

| | |
|---|---|
| **Resources** | EnCycLEd Guides + Module 5 "Cyberpeace"; chart paper or digital collaboration board. |
| **Lesson Flow (Steps)** | **Session 1:** Identify unsafe behaviours (sharing passwords, online gossip). Discuss consequences. **Session 2:** Create a "Cyber Citizen Charter" – 5 golden rules for school's online culture. Optional: display charter on classroom wall or school website. |
| **Expected Outcome** | Students internalise ethical principles and demonstrate collective responsibility for online conduct. |
| **Teacher Tips** | Focus on empathy and respect. Use real-life scenarios (e.g., "What if someone shares a private photo?"). Let students propose solutions rather than rules from adults. |

*Table 45: Activity 4 – "Cyber Citizen Challenge" (all ages).*

| Element | Description |
|---|---|
| **Goal** | Consolidate learning from all modules and Guides through teamwork, creativity, and presentation. |
| **Duration** | 2–3 weeks (preparation + event day) |
| **Methodological Focus** | Project-based learning, public speaking, synthesis of cyber hygiene knowledge and career understanding. |
| **Resources** | All EnCycLEd Modules + Guides; materials for posters, games, or digital booths. |
| **Lesson Flow (Steps)** | **1. Plan:** Assign teams (each represents one module or cyber role). **2. Create:** Students design interactive stands (e.g., "Phishing Game Zone", "Cyberpeace Corner", "Meet the Ethical Hacker"). **3. Present:** Organise school fair for peers and parents. **4. Reflect:** Group discussion – "What did we learn about teamwork and protecting others online?" |
| **Expected Outcome** | Students demonstrate holistic understanding of cybersecurity and pride in being digital citizens. |
| **Teacher Tips** | Involve parents or younger pupils to create mentoring effect. Use rubrics for creativity, accuracy, and cooperation. Celebrate achievements – small certificates or badges strengthen motivation. |

*Table 46: Activity 5 – "Cyber Career Fair".*

For a full list of classroom and extracurricular activities using the Guides, see *Program Development Section 5.3 "Using Guides materials for career guidance and extracurricular activities".*

### Methodologist's Advice

- **Emphasise values before vocation.** Students must first understand *why* cybersecurity matters to people's safety.

• **Build emotional connection.** Let them feel pride in protecting friends and family online – this builds intrinsic motivation.

• **Show diversity of talents.** Use role cards: "The Creator", "The Detective", "The Guardian", "The Communicator" – each linked to a cyber role.

• **Encourage reflection.** Every activity should end with the question: *"What can I do right now to make the digital world safer?"*

**Expected Learning Outcomes**

After completing career-oriented lessons with Guides, students will:

1. Understand that **cyber hygiene and careers share the same values** – awareness, responsibility, and teamwork.
2. Recognise at least **three distinct cybersecurity roles** and what skills they require.
3. Be able to **connect school subjects to digital professions**.
4. Express **respect and curiosity** toward both genders and diverse career paths in technology.

Demonstrate **motivation to learn and act safely online** – the foundation of a future cyber-resilient generation.

# SECTION 9 - ASSESSMENT, MEL, AND LESSON ORGANISATION

Assessment in EnCycLEd is not about grading – it is about measuring awareness and growth. The MEL approach (Monitoring – Evaluation – Learning) focuses on how students think, act, and feel about cyber safety before and after participating in modules. Teachers collect only light, anonymous evidence to see progress and improve their own practice.

## 9.1 Pre / Post (Minimal Forms)

**Purpose:** to capture students' baseline knowledge and changes in attitude after completing the modules.

| Stage | Form Type | Example Questions | Teacher Action |
|---|---|---|---|
| **Pre-Lesson (Before Module 1)** | 2-question warm-up | 1. What does "cybersecurity" mean to you?<br>2. Name one online risk. | Collect answers verbally or on post-its. |
| **Mid-Point (Between Modules 3–4)** | Reflection check-in | "What has changed in the way you use the Internet?" | 5-min quick discussion. |
| **Post-Lesson (After Module 5)** | 4-question exit form | 1. One thing I learned about staying safe online is…<br>2. Now I can explain what a phishing message is.<br>3. I feel more confident to protect my data (Yes/No).<br>4. My favourite activity was … | Review for patterns (not scores). |

*Table 47: Minimal Forms.*

## 9.2 Mini-Quizzes / Final Quiz

**Purpose:** to reinforce learning and offer instant feedback through playful assessment.

| Type | Timing | Format and Examples | Learning Focus |
|---|---|---|---|
| **Mini-Quiz** | End of each module | 3–5 short questions (Kahoot, paper cards, or verbal). e.g. "What is a digital footprint?", "Name two safe password habits." | Recall core concepts. |
| **Peer Quiz** | During group work | Students create their own questions and quiz others. | Deepen understanding through teaching others. |
| **Final Quiz** | After Module 5 | 8–10 questions covering Modules 1–5. Example sections: Hygiene ✓ Incidents ✓ Resilience ✓ Defense ✓ Ethics. | Consolidate global knowledge. |

*Table 48: Quizzes.*

## 9.3 Methods: Individual Study, Interactive, Group Work, Educational Game

A balanced lesson combines thinking, doing, and reflecting. Teachers should alternate methods to keep motivation and reach different learning styles.

| Method | Description | Age Suitability | Example Activity | Why It Works in Cyber Hygiene Education |
|---|---|---|---|---|
| **Individual Study** | Reading articles or working on personal worksheets. | All | "My Digital Footprint" worksheet. | Builds self-awareness and responsibility. |
| **Interactive Discussion** | Teacher-led conversation or quiz with instant answers. | All | "Myth or Fact?" about passwords. | Corrects misconceptions quickly. |
| **Group Work** | Team tasks requiring collaboration and role play. | 10–17 | "Who was it?" cyber investigation. | Encourages peer learning and communication. |
| **Educational Game** | Digital or tabletop games simulating decisions. | 10–18 | *Cyber Crime Time*, *Google Interland*. | Converts theory into experience; safe trial and error. |

*Table 49: Methods.*

## 9.4 Classroom Logistics and 45-Minute Timing

A well-structured lesson ensures focus and flow. Below is a recommended time allocation model for a 45-minute session.

| Phase | Time | Teacher Action | Student Action | Outcome |
|---|---|---|---|---|
| **0 – Introduce** | 5 min | Welcome and question hook ("What keeps you safe online?") | Share ideas | Connect to real life. |
| **1 – Explore** | 10 min | Present video/comic, explain 2 key terms | Listen + note examples | Understand concept. |
| **2 – Apply** | 20 min | Facilitate activity or game | Work individually or in teams | Practise decision-making. |
| **3 – Reflect** | 8 min | Summarise + ask "What will you do differently?" | Answer or write on cards | Internalise lesson. |
| **4 – Wrap Up** | 2 min | Mini-quiz or thank-you note | Quick feedback emoji 🙂😐☹️ | Record insight. |

*Table 50: Classroom Logistics.*

## 9.5 Inclusivity and Accessibility of Materials

**Principles:** EnCycLEd lessons follow universal design for learning (UDL) – ensuring every student can participate fully, regardless of language level, gender, or digital access.

| Aspect | Recommended Practice | Why It Matters |
|---|---|---|
| **Language Accessibility** | Use simple vocabulary, translate key terms on board (Ukrainian + English). | Helps ELL and younger learners grasp concepts. |
| **Visual Support** | Add icons and infographics for abstract concepts (e.g., lock = security). | Visual memory enhances retention. |
| **Gender Balance** | Use equal examples of men and women in cyber roles. | Encourages inclusive role modelling. |
| **Differentiated Tasks** | Provide simpler or extended versions of worksheets. | Maintains engagement for mixed-ability groups. |
| **Participation Choice** | Allow oral answers, drawings, or short notes instead of writing essays. | Reduces anxiety and fosters expression. |
| **Accessibility Tools** | Offer large-font materials, captions for videos, screen reader compatibility. | |

*Table 51: Inclusivity and Accessibility.*

## 9.6 KPI Dashboard Summary for Teachers

### Purpose

This section provides a concise overview of how classroom activities contribute to the overall EnCycLEd project indicators. The KPI Dashboard enables teachers and coordinators to easily monitor progress, record results, and understand how their class-level work contributes to the project's broader goals and evaluation (Deliverables D4.3–D4.4). It also simplifies reporting at the end of the pilot cycle.

### Instructions for Use

Each teacher records the actual results at the end of the pilot (or after each module if preferred). Values can be expressed as percentages, counts, or brief comments. The final table is attached to the One-Page School Summary Report (Section 11.1).

| Indicator | My Class Target | My Actual Result | How to Report |
|---|---|---|---|
| **Students completed all modules planned in the school's piloting package (A, B, or C)"**<br>**Target: 100% of students in participating classes complete the planned modules** | 100% | … | Final report (Section 11.1) |
| **Average quiz improvement** | 30% | … | Quiz forms (Pre/Post results) |
| **Participation in joint cross-learning session** | 1 event | … | Section 11.3 (Cross-Learning Summary) |
| **Female participation** | ≥40 % | … | Class log / attendance list |
| **Student reflections submitted** | 100% | … | Lesson folder / reflection cards |
| **Teacher satisfaction and confidence** | ≥4/5 | … | Teacher reflection note |

| | | | |
|---|---|---|---|
| **Student engagement (high/medium/low)** | ≥80 % high | … | Lesson observation notes |
| **Technical issues encountered** | ≤10 % of sessions | … | Short note in reflection log |

*Table 52: KPI Dashboard Template.*

**Notes**

- Data are indicative and used **only for educational evaluation**, not for ranking.
- Percentages can be estimated based on class participation.
- Qualitative observations (e.g., *"Students showed increased interest after Module 3"*) are also valuable and should be added in the comments.
- Reports remain anonymous and in line with GDPR standards.

**Methodological Recommendation**

The KPI Dashboard helps visualise progress and impact. When completed consistently, it supports transparent monitoring at school, national, and European levels, demonstrating real learning outcomes achieved through EnCycLEd piloting.

## 9.7 Timeline and Completion of Piloting-Related Assessment

All assessment and monitoring tools described in this section (pre/post forms, mini-quizzes, teacher reflections, lesson observations) are part of the **overall piloting package** and must be scheduled within the same time window as the teaching activities themselves.

When preparing their **National Piloting Calendar**, partners should explicitly mark:

- when pre-pilot baselines will be collected;
- when module-level quizzes and classroom observations will take place; and

- when post-pilot forms and final reflections will be gathered from teachers and students.

This helps ensure that all MEL data required for EnCycLEd indicators are collected **before the national piloting period ends**, leaving **1–2 months** for partners to clean, aggregate, and interpret the data and to contribute to the project-wide Evaluation and Cross-Learning deliverables. Assessment, in other words, is not an "add-on" after the pilot, but a planned component of the piloting calendar itself.

**Internal reporting deadlines for piloting**

To allow enough time for cross-country evaluation before the project end, the consortium has agreed the following internal deadlines:

**By 30 June 2026** – piloting schools complete the School Piloting & KPI Report (Annex E1) and send it to their national coordinator.

**By 15 July 2026** – national coordinators submit the National Piloting Synthesis Report (Annex E2) to UACS (WP4 lead).

**By 31 July 2026** – AC and UACS finalise platform usage and Discussions data (Annex E3) and complete the Master KPI WP4 Dashboard (Annex E4).

These internal dates should also be reflected in the National Piloting Calendar Template (Annex E8) as default deadlines, unless an earlier national deadline is agreed

**Outcome of Section 9**

After applying this assessment and lesson organisation framework, teachers will be able to:

1. Monitor students' progress through light, non-intrusive evaluation.
2. Adapt instruction to different learning styles and abilities.

3. Create safe, inclusive and motivating learning spaces.

Foster not only knowledge but also attitudes and habits of responsible digital citizenship.

# SECTION 10 - SAFETY, PRIVACY, AND ETHICS

Teaching cybersecurity goes beyond technology – it's also about modelling digital responsibility. Teachers must protect students' privacy, promote ethical online conduct, and ensure that all digital learning tools are used safely and transparently.

This section provides clear guidance on handling student information, using external online resources, and embedding digital ethics in everyday teaching practice.

## 10.1 Student Data and Consent

### Core Principle

No personal data from students should ever be collected, stored, or shared as part of the EnCycLEd pilot. All activities must respect data minimisation, anonymity, and informed participation, in line with the General Data Protection Regulation (GDPR) and national education laws.

| What Is Collected | Purpose | How to Handle |
|---|---|---|
| **Non-identifiable feedback (e.g., "I liked the video")** | Evaluate engagement | Anonymous sticky notes or forms |
| **Quiz answers (without names)** | Measure learning outcomes | Aggregated summary (e.g., % of correct answers) |
| **Teacher reflections** | Internal improvement | Stored locally by the teacher only |
| **Screenshots (optional)** | Evidence of activity | Use only if no student faces/names visible |

*Table 53: Minimal Data Collection.*

### Consent and Communication

- **Under 14 years old:** Always inform parents or guardians in advance when digital tools, videos, or online games are used.

- **Parent/guardian letter:** Include purpose, safety assurance, and clarification that no personal data are stored.

• **Student awareness:** Explain to children *why* we protect data – link it to their own digital safety (e.g., "Just like you wouldn't post your home address online, we also keep your class work private.")

**Sample statement for classroom use:**

"In this project, we don't use our real names online, and we don't share personal details. Our goal is to learn how to stay safe – not to collect data."

| Area | Teacher Practice | Reason |
|---|---|---|
| **Student Identity** | Use first names or nicknames only in digital tools. | Prevent traceability. |
| **Photo/Video Use** | Obtain written consent before publishing any images. | Comply with GDPR. |
| **Cloud Storage** | Save student work on school servers, not public drives. | Ensure data control. |
| **Email/Accounts** | Never create accounts for students under your name. | Maintain transparency. |

*Table 54: Teacher Responsibilities.*

**TIP:** Treat student data the same way you teach them to treat their own: carefully, consciously, and with respect. Each teacher's example sets the ethical tone for the classroom.

## 10.2 Use of External Services and Games

External services (videos, games, simulations) can greatly enrich cybersecurity learning – but they must be checked for safety, relevance, and data protection before use.

| Step | Action | Example |
|---|---|---|
| 1 | **Check source credibility.** Use only educational or official sites. | ENISA, Google Interland, Cyber Crime Time, Better Internet for Kids. |
| 2 | **Preview content.** Ensure all links work and there is no advertising or harmful content. | Watch or play once before class. |
| 3 | **Avoid personal login.** Use guest or demo modes where possible. | Students play without creating accounts. |

| | | |
|---|---|---|
| 4 | **Use offline backup.** Prepare screenshots or printed worksheets in case of blocked access. | Print 3–5 key slides for discussion. |
| 5 | **Never share results publicly.** Quizzes or game scores stay within the class. | Discuss learning, not rankings. |

*Table 55: Safe Use Policy.*

| Age Group | Suitable Content | Avoid |
|---|---|---|
| **10–14 years** | Simple games, comics, basic definitions, short videos (<5 min). | Complex simulations, registration-required platforms. |
| **15–18 years** | Analytical case studies, strategic games, ethical debates. | Content involving data entry or external messaging. |

*Table 56: Age-Appropriate Guidelines.*

## Ethical Classroom Practice

When using digital tools, model the same ethical behaviour expected from students:

- Always cite sources of videos or materials.
- Discuss copyright and fair use – even short YouTube clips should include credits.
- Reinforce respectful online communication (no mocking, no screenshots of peers).
- Encourage digital empathy – think before posting or commenting.

## Ethics Prompt for Class Discussion:

"If I wouldn't say it in real life, I shouldn't write it online." "If I share someone's content, do I have their permission?"

| ✅ Preparation | 💬 During Lesson | 🛡️ After Lesson |
|---|---|---|
| **Check Wi-Fi and firewall access to required pages.** | Remind students not to enter personal data online. | Close all tabs and clear browsing history. |
| **Review external links and privacy policies.** | Monitor screen use – ensure safe behaviour. | Delete any temporary files or screenshots. |



Co-funded by the European Union

| | | |
|---|---|---|
| **Prepare offline materials as backup.** | Use group discussions rather than individual accounts. | Store teacher notes locally (not cloud-shared). |

*Table 57: Teacher's Safety Checklist (Before Each Lesson).*

### Teaching Digital Ethics Through Practice

Integrate short ethics reflections in every lesson:

- **After a game:** "Was every decision in the game fair or ethical?"
- **After watching a video:** "Would you share this video with a friend? Why or why not?"
- **After group work:** "What does it mean to respect each other's digital space?"

These moments build critical thinking, empathy, and moral awareness – the foundation of safe online citizenship.

### Key Takeaways for Teachers

1. Protecting privacy in class teaches privacy by example.
2. Always test tools before use – trust, but verify.
3. Create a culture of mutual respect and consent – every student's data and opinion matter.
4. Digital ethics are caught, not taught – students learn them by observing you

# SECTION 11 - REPORTING AND HANDOVER OF RESULTS

The goal of EnCycLEd reporting is not only to document classroom results, but also to create an international learning community. By sharing experiences across schools and countries, teachers and students co-develop a European understanding of cybersecurity education and digital citizenship.

## 11.1 School Report Formats (Monthly / Term)

Each participating school compiles short reports that capture successes, challenges, and local adaptations. These reports form the foundation for **cross-country reflection sessions** (see Section 11.3 below).

## 11.2 Data Aggregation for Pilot Partners

National partners analyse teacher feedback and compile aggregated insights. This data is then used to identify patterns of innovation worth sharing across borders.

The schedule for school reports and national aggregation should follow the **National Piloting Calendar** agreed in each country. By anchoring reporting deadlines in this calendar, partners can verify that:

- schools have enough time after completing their modules to finalise their reports;
- national teams can review and consolidate data from all piloting schools; and

National piloting reports should be submitted to the consortium **by 31 July 2026**, so that cross-country evaluation and sustainability assessment (**31 July – 15 October 2026**) can be completed in line with the project Gantt chart.

## 11.3 Cross-Learning and International Exchange

The aim of cross-learning is to promote mutual learning, peer support and intercultural collaboration between teachers and students in the EnCycLEd pilot. It

strengthens both digital skills and European values such as cooperation, empathy and respect for diversity.

### Discussions as a space for cross-learning

The *Discussions section* is the default online environment for cross-learning and international exchange during piloting. It provides a safe, moderated space where:

- students can share experiences and outputs across countries (e.g. comparing class rules, posters, or campaigns);
- classes can follow up after virtual joint lessons, continuing the discussion asynchronously;
- international cyber hygiene challenges and campaigns can be coordinated and documented.

Partners are encouraged to plan cross-learning activities so that they are anchored in specific Discussion Groups, created and moderated by teachers in line with the Behaviour and Safety Policy (see Section 2).

The *Discussions section* can be used to:

- host cross-country discussion threads on common topics (e.g. a Module 5 "Cyberpeace" question, or a joint cyber hygiene challenge);
- support joint projects (e.g. groups from different schools share drafts of class charters, posters or campaigns, and provide feedback to each other);
- run asynchronous Q&A sessions with cybersecurity professionals, where students from several countries post questions and read the answers.

These activities **should be** explicitly included in the **National Piloting Calendars** (for example: *"Week X – joint Discussion on cyberbullying with School Y in Country Z"*) and reported as part of the piloting KPIs related to cross-country exchange and use of the platform. When reporting on piloting and cross-learning, partners should

also describe how the Discussions section was used (within classes, across countries, and with guest professionals); practical guidance on setting up and running these online exchanges is provided in Section 2.

Partners may design additional formats, as long as they:

- involve students from at least two different countries, and
- are run through the Discussions section (or, where this is not technically possible, are clearly documented if another secure platform is used).

At project level, it is strongly recommended that each partner organises at least one cross-learning activity via the Discussions section during the piloting period, in order to meet the D4.5 cross-learning KPIs and to generate rich qualitative evidence for the final cross-learning and sustainability reports.

| Format | Description | Tools / Platform | Frequency |
|---|---|---|---|
| **Virtual Joint Lessons** | Mixed-country online sessions where teachers co-teach the same module (e.g., "Cyberpeace"). | Zoom / Google Meet / eTwinning / EnCycLEd Hub | Once per semester |
| **Teacher Exchange Workshops** | Online or hybrid meetings to discuss pedagogy, assessment, and classroom experiences. | EnCycLEd Forum / Padlet / Miro | Quarterly |
| **Student-to-Student Sharing** | Joint online activities or video messages where learners explain what they discovered. | Shared Padlet or short recorded clips | After Module 3 and 5 |
| **International Cyber Hygiene Challenge** | Friendly quiz or creative campaign across schools ("Design a Digital Safety Poster Together"). | Kahoot / Canva / Mentimeter | Once per project year |
| **Peer Mentoring Circles** | Teachers mentor teachers; older students mentor younger ones abroad. | Google Classroom / shared Drive | Optional, ongoing |

*Table 58: Forms of Cross-Learning.*

## Learning Outcomes

- **For Students:**

o Broaden cultural awareness and digital empathy.

o Recognise common cyber challenges faced by peers in other countries.

o Build communication skills in English while discussing technical topics.

- **For Teachers:**

o Gain fresh classroom ideas and adaptable strategies.

o Compare teaching methods and resource use.

o Strengthen confidence in cross-cultural digital education.

| Step | Action | Responsible |
|---|---|---|
| **1. Matchmaking** | National partners connect schools interested in cross-learning. | EnCycLEd country coordinators |
| **2. Co-Planning** | Teachers agree on shared module (e.g., Module 5 – *Cyberpeace*). | Participating teachers |
| **3. Joint Lesson Delivery** | 30–45 min online session with both classes (intro + joint activity + reflection). | Teachers + students |
| **4. Reflection & Sharing** | Students write short feedback sentences ("What I learned from another country"). | Teachers collect reflections |
| **5. Reporting** | Include summary in school's final report ("Joint lesson conducted with partner school in Spain / Malta / Greece"). | Teachers |

*Table 59: Implementation Steps.*

Cross-learning results are evaluated using qualitative indicators.

| Indicator | Evidence Example |
|---|---|
| **Engagement in international session** | Attendance list or screenshot (no student faces) |
| **Intercultural awareness** | Student quotes comparing habits or rules ("We also talk to parents about passwords.") |
| **Collaboration quality** | Teacher reflections on group dynamics |
| **Pedagogical innovation** | New method or resource inspired by another country's example |

*Table 60: Evaluation and Integration into MEL Framework.*

## Ethical and Logistical Considerations

- Obtain parental consent before any cross-country video participation.
- No personal information or full-face images of students are shared.
- Use school accounts, not personal ones, for online sessions.
- Keep sessions under 45 minutes with clear learning goals.
- Promote respectful communication – include 2 minutes for digital-etiquette reminders at the start.

| Aspect | Reflection Prompt |
|---|---|
| **Collaboration setup** | How did you coordinate with the partner teacher? |
| **Student reactions** | What surprised or excited your students most? |
| **Learning insight** | What did both classes learn from each other? |
| **Next steps** | How can this partnership continue beyond the pilot? |

*Table 61: Teacher Reflection Template (for Cross-Learning).*

## Expected Impact

- Strengthened European network of cyber educators.
- Increased student motivation through real peer connections.
- Shared understanding of cyber hygiene as a global, human value, not only a technical topic.
- Creation of an informal Community of Practice (CoP) – teachers continue sharing resources even after the pilot ends.

**Methodologist's Advice**

Cross-learning is where cybersecurity education becomes alive. When students in Ukraine, Greece, and Malta discuss how they protect their devices, they don't just learn – they build digital empathy and a European identity of shared responsibility online.

Encourage every teacher to participate in at least one international activity per semester. Even a 30-minute shared quiz can create lasting curiosity and pride.

## 11.4 Feedback Loop and Sustainability

The feedback loop ensures that insights and experiences gathered during the EnCycLEd piloting phase are continuously integrated into the project's improvement process. This approach aligns with Erasmus+ quality assurance requirements and contributes directly to Deliverables D4.4 (Evaluation and Impact Report) and D4.6 (Policy and Practice Recommendations). It guarantees that the pilot outcomes are not limited to the project cycle but remain available, relevant, and usable beyond 2026. The feedback loop described in this section is activated on the basis of the **National Piloting Calendars** and associated reporting deadlines, so that insights from each country can be discussed, compared, and integrated into the final project outputs within the overall EnCycLEd timeline.

**A. Post-Pilot Evaluation Process**

After the completion of national piloting activities and submission of all country reports, EnCycLEd partners will organise a joint online evaluation meeting.
The purpose of this meeting is to:

- Review the lessons learned and analyse the most effective teaching practices;
- Discuss technical and pedagogical improvements for the EnCycLEd platform;
- Identify successful local adaptations for potential EU-wide scaling;
- Validate preliminary findings included in Deliverable D4.4 (Evaluation Report)

Each partner will present a short summary of results from participating schools, including examples of:

- effective classroom integration,
- cross-learning activities,
- and innovative teaching methods that enhanced student engagement.

**B. Teacher and School Acknowledgement**

All schools and teachers who participated in the pilot will receive a Digital Certificate of Contribution issued jointly by the EnCycLEd Consortium. The certificate will acknowledge the participant's contribution to:

- advancing cybersecurity education in schools;
- supporting the validation of European teaching materials;
- contributing to international cooperation and research-based educational improvement.

Certificates will be distributed electronically through national partners after verification of final reports.

**C. Updating and Maintaining Resources**

Following the evaluation phase, the consortium will:

1. Integrate teacher feedback and evaluation data into an updated version of the Teacher Toolkit and Playbook (Modules 1–5).
2. Upload all revised and validated materials to the EnCycLEd platform — https://go.EnCycLEd.eu.
3. Maintain public access to educational resources for at least two years beyond the project's official end (until 2028).

4. Encourage schools and teachers to continue using, translating, or expanding these resources under the project's open educational license (CC BY-NC-SA 4.0).

**D. Knowledge Sharing and Long-Term Impact**

To ensure sustainability and continuous growth of the EnCycLEd community:

● A Community of Practice (CoP) will be established, connecting teachers, schools, and organisations that took part in piloting.

● Annual online exchange sessions will be organised to share new materials, classroom stories, and best practices.

● Teachers will be invited to contribute to new editions of the *Cybersecurity in Education Guidebook* (2026–2027).

● Schools will be encouraged to integrate EnCycLEd modules into regular ICT, citizenship, and digital competence curricula.

The feedback loop creates a living ecosystem of knowledge within EN-CYCLED. By systematically collecting reflections, validating outcomes, and improving materials, the project ensures that the piloting phase evolves into a sustainable educational model. This process guarantees long-term impact and continuous relevance of cybersecurity education across Europe, in line with Erasmus+ sustainability principles.

By combining structured reporting with reflective, cross-border learning:

1. Teachers contribute to both national and international impact data.
2. Students experience cybersecurity as a shared European challenge and opportunity.
3. EnCycLEd builds a sustainable network of educators who continue to teach, mentor, and learn together long after the pilot ends.

## Conclusions

This Piloting Program Guide provides a common framework for all EnCycLEd partners to organise, support and evaluate piloting activities in a coherent way. It clarifies what is expected from piloting schools and higher education partners, how their classroom and platform activities map onto project KPIs and deliverables, and how data from different countries will be combined in the Cross-Country Evaluation & Sustainability Assessment (Task 4.6).

The Guide emphasises flexibility within clear boundaries. Schools can select between minimum piloting packages (Options A, B or, in exceptional cases, C), but are expected to reach the agreed minimum numbers of students and teachers involved, platform registrations, use of the Discussions section, and cross-country activities as set out in the annexes. National Piloting Calendars, together with the internal reporting deadlines (school reports by 30 June 2026, national synthesis by 15 July 2026, and all data to WP4 by 31 July 2026), ensure that piloting activities finish early enough for meaningful cross-country evaluation and final reporting.

Following discussion and fine-tuning at the Malta workshop, the consortium agreed that this Piloting Program Guide, together with its annexes (minimum piloting packages, KPI and partner targets, and the National Piloting Calendar Template), will serve as the single internal point of reference for planning, implementing and reporting EnCycLEd piloting. Any later adjustments to piloting arrangements or targets should be agreed with WP4 (UACS) and reflected in updated versions of this Guide and its annexes. For day-to-day lesson delivery and classroom activities, teachers should continue to use this Guide in combination with the Program Development document, which remains the primary reference for module content, classroom methods and concrete teaching examples.

# ANNEX A

## For Schools – At a Glance

### EnCycLEd Piloting – What Your School Is Expected to Do

This page explains, in simple terms, what is expected from your school during the EnCycLEd piloting. Please read it together with the **Piloting Program Guide** and the **Program Development** document.

### 1. Your choice of piloting "package" (Options A, B, or C)

Each piloting school should choose **one of three options**. This helps everyone plan realistically while still meeting the project's goals.

### Option A – Full package (recommended for main piloting schools)

Your school delivers:

- **All 5 EnCycLEd modules** (Modules 1–5) to at least one class or group.
- At least **1 structured activity using the Guides** (Cybersecurity Careers and Study Pathways).
- At least **50–60 students** participate in the piloted modules.
- Students are **registered on the Platform** according to your target (e.g. AFS 250, SU 200, KVS 250).
- At least **3 uses of the "Discussions" section**, e.g.:
  - a short reflection thread after a module,
  - a cross-country discussion with another school,
  - a Q&A with a cybersecurity professional.

**Option B – Core package**

Your school delivers:

- At least **3 modules**, including:
  - **Module 1** (intro),
  - **one technical module** (2, 3 or 4),
  - **Module 5 (Cyberpeace)**.
- At least **1 activity using the Guides**.
- At least **30–40 students** participate.
- Students are registered on the Platform towards your target numbers.
- At least **2 uses of "Discussions"** (e.g. reflection + cross-country/Q&A).

**Option C – Light package (exceptional)**

This is only for **special cases** (e.g. late entry, smaller additional schools) and must be agreed with the **WP4 lead (UACS)** and your **national coordinator**.

Your school delivers:

- At least **1 module**,
- At least **1 Guides-based activity**,
- At least **20–30 students** participate,
- At least **1 use of "Discussions"**.

## 2. Key numbers ("KPIs") your school contributes to

You do **not** need to memorise all codes, but it helps to know what will be counted.

For each piloting school, we look especially at:

- **How many students and teachers are directly involved** in piloting (K1)
    - AFS: **≥ 60** | SU: **≥ 50** | KVS: **≥ 50**
- **How many teachers are registered on the Platform** (K2)
    - AFS: **33** | SU: **33** | KVS: **33**
- **How many students are registered on the Platform** (K3)
    - AFS: **250** | SU: **200** | KVS: **250**
- **How many other teachers you inform about the Platform** (K4)
    - At least **50** per piloting school (e.g. via staff meetings, emails).
- **How many students you inform about the Platform** (beyond those piloting) (K5)
    - AFS: **500**, SU: **400**, KVS: **500** (e.g. assembly, campaign, posters).
- **How you use the "Discussions" section** (D1–D7)
    - Each piloting teacher uses Discussions at least once.
    - Your school participates in **at least one cross-country Discussion** (e.g. joint thread or virtual exchange).
    - Students post, reply and ask questions – we will also collect a short description of what kinds of exchanges took place.

## 3. Timelines – when your school reports

To allow enough time for cross-country evaluation:

- By **30 June 2026** – your school sends its **piloting report** and fills in the simple KPI table (we will provide a template).

- Your national partner then combines your data with other schools and reports at country level.

- The consortium analyses everything between **31 July and 15 October 2026**. You will receive **templates and guidance** so that reporting is as simple and light as possible.

# ANNEX B

## Piloting Schools KPIs

The table below sets out the **minimum targets** that each piloting school (AFS, SU, KVS) is asked to reach during the piloting period. These are **internal planning targets** agreed by the consortium, to make sure we all contribute fairly to the project goals and to the commitments in the EnCycLEd proposal.

**K1–K5:**

*Piloting schools and HEIs are responsible for achieving the minimum numbers in K1–K5; UACS aggregates these numbers, and REACH uses them for dissemination and sustainability.*

**K6–K7 (cross-country):**

*Piloting schools and HEIs are responsible for planning and running cross-country teams and sessions (K6–K7); AC supports the technical set-up and provides usage data; UACS uses this evidence in the cross-learning evaluation (D4.5).*

**D1–D7 (Discussions KPIs):**

*Teachers and students in piloting schools and HEIs are responsible for using the Discussions section (D1–D4); AC logs usage; UACS and REACH interpret and communicate the qualitative aspects of these exchanges (D5–D7).*

| KPI ID | KPI Description | Unit | AFS Min | SU Min | KVS Min | Notes for Schools |
|---|---|---|---|---|---|---|
| K1 | Number of teachers and students involved in piloting (direct participants) | # persons | 60 | 50 | 50 | Total number of teachers **plus** students directly involved in piloted lessons and activities. |
| K2 | Number of teachers (and future teachers) | # teachers | 33 | 33 | 33 | Teachers with active accounts on **go.encycled.eu** who |

| | | | | | | |
|---|---|---|---|---|---|---|
| | registered on the Platform | | | | | will use the Modules / Guides / Discussions during piloting. |
| **K3** | Number of students registered on the Platform | # students | 250 | 200 | 250 | Students with accounts on **go.encycled.eu** (where applicable) who will participate in piloting activities. |
| **K4** | Number of other teachers / future teachers informed about the Platform (non-registered) | # teachers informed | 50 | 50 | 50 | Teachers informed about EnCycLEd and the Platform (e.g. through staff meetings, newsletters, short presentations), even if they do not register. |
| **K5** | Number of students informed about the Platform (beyond those registered) | # students informed | 500 | 400 | 500 | Students who hear about EnCycLEd / the Platform (e.g. assemblies, campaigns), **in addition** to those registered as users. |
| **K6** | Cross-country teams formed and interacting on the Platform | # teams (school contribution) | ≥ 1 teacher team + ≥ 1 student team | ≥ 1 teacher team + ≥ 1 student team | ≥ 1 teacher team + ≥ 1 student team | Each school participates in at least one cross-country **teacher team** and one **student team** (exact matching to be agreed with partners). |
| **K7** | Cross-country learning and exchange sessions hosted on the Platform | # sessions (school contribution) | ≥ 1 | ≥ 1 | ≥ 1 | Each school participates in at least one cross-country learning / exchange activity (e.g. joint Discussion, shared project, online session). |
| **D1** | Teachers using Discussions section | # teachers using Discussions | All piloting teachers | All piloting teachers | All piloting teachers | All teachers involved in piloting should use the **Discussions** section at least once with their classes. |
| **D2** | Discussion Groups created for piloting | # Groups (school contribution) | ≥ 2 | ≥ 2 | ≥ 2 | At least two Discussion Groups per school (e.g. one **class reflection** group + one **cross-country / Q&A** group). |
| **D3** | Cross-country Discussion Groups | # cross-country Groups (school contribution) | ≥ 1 | ≥ 1 | ≥ 1 | Each school participates in at least one **cross-country** Discussion Group with a partner school in another country. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **D4** | Students registered in Discussion Groups | # students in Discussions | Subgroup of 250 | Subgroup of 200 | Subgroup of 250 | At least one piloted class per school has students registered in a Discussion Group; exact numbers defined in national planning / piloting calendar. |
| **D5** | Guest cybersecurity professionals / role models engaging with the school via Discussions or events | # guest professionals (school contribution) | ≥ 1 (where feasible) | ≥ 1 (where feasible) | ≥ 1 (where feasible) | Each school is encouraged to host at least one Q&A or interaction with a cybersecurity professional (online or onsite), possibly shared with other schools. |
| **ME 1** | Participation in piloting-related dissemination / school events | # events / contributions | ≥ 1 | ≥ 1 | ≥ 1 | Each school contributes to at least one event or activity showcasing piloting results (e.g. school fair, open day, national or online event). |

*Table B1: KPI.*

**Note for Piloting Schools:**

In simple terms, the table shows for each KPI:

- **What we count** – for example, number of students involved, teachers registered on the Platform, Discussion Groups created, cross-country activities, etc.
- **The minimum numbers per school** – columns "AFS Min", "SU Min", "KVS Min".
- **What this means in practice** – short notes for schools in the last column.

These minima are **not meant to add bureaucracy**, but to help you:

- plan the size and scope of piloting (how many classes, how many teachers);
- include at least **one cross-country activity** and **meaningful use of the Discussions section**;

- show that piloting also supports **career guidance** and **school-level events**.

**How you will report these figures**

Each piloting school will complete a **short School Piloting Report and KPI table** at the end of its piloting period (templates will be provided by the national coordinator / WP4).

The **school coordinator** (or contact person for EnCycLEd) will collect the numbers for your school from:

- class lists and lesson plans (participants, modules delivered),
- Platform statistics (teachers/students registered, Discussion Groups),
- simple logs of cross-country activities and events.

Your national/project partner will then prepare a **country-level synthesis**, and WP4 (UACS) will use these summaries for the **cross-country evaluation and lessons learned**. If you see that you will **easily exceed** the minimum numbers, that is excellent – please still record the full figures. If you have doubts about reaching any minimum target, please contact your **national EnCycLEd coordinator** early, so we can adjust plans together.

# ANNEX C

## EnCycLEd National Piloting Calendar Template

The National Piloting Calendar template is intended for **piloting partners / educational institutions** who deliver modules and classroom activities. It does not apply to partners whose role is primarily technical support, evaluation or coordination (e.g. AC, REACH), who have separate commitments and timelines.

**EnCycLEd – National Piloting Calendar**

**Country:** _____ **Partner:** _____

**Academic year/term:** _____

**Responsible person (s) Nat. partner / school lead** _____

**Piloting window (school level):** ___ / ___ / 20__ – ___ / ___ / 20__

**School report deadline to national partner:** ___ / ___ / 20__

**National report deadline to consortium:** ___ / ___ / 20__

**Reminder:** All piloting activities and deliverables must finish before 30 Nov 2026, with piloting ending 1–2 months earlier.

| Week # | Dates (from –to) | Main piloting activities (schools) | Platform use (Modules / Disc. / Guides) | Data & KPIs | Notes / reporting |
|---|---|---|---|---|---|
| 1 | __ / __ / __ – __ / __ / __ | Select piloting classes and confirm timetable; introduce EnCycLEd to students; explain objectives, consent and basic ground rules. | Teachers explore Platform; show students the structure (Modules, Resources, Glossary, Guides, Links, Discussions); no login yet or only teacher login. | Collect baseline info on schools/classes/teachers (simple template); note number of participating teachers and classes; record planned number of students. | |

| | | | | | |
|---|---|---|---|---|---|
| **2** | __ / __ / __ – __ / __ / __ | Deliver introductory lesson using Module 1 (why cybersecurity and digital citizenship matter); set simple homework or reflection task. | Use Module 1 materials in class; show relevant Resources and Glossary entries; teacher posts a first message in a class Discussion room (if access already set up). | Apply pre-test / baseline questionnaire for students (if applicable); log which classes completed Module 1; note number of students reached. | |
| **3** | __ / __ / __ – __ / __ / __ | Continue Module 1 or start Module 2 (technical / hygiene focus) depending on timetable; small group activities in class. | Use Module 2 on Platform for exercises or case studies; encourage students to check Resources at home (no sign-in needed); open class Discussion thread for "questions to the teacher". | Teacher logs completion of Module 1 and start of Module 2; simple count of active classes and approximate student participation; note first questions/posts in class Discussion threads. | |
| **4** | __ / __ / __ – __ / __ / __ | Deliver next lesson(s) from Module 2 and/or begin Module 3 (e.g. cyber threats, scenarios, or games); invite students to share examples from their own experience. | Use Modules 2–3 and relevant games/activities; ask students to post 1 short example or question in the Discussion room after class; test basic moderation practices. | Tally number of posts and comments in class Discussions; record which modules/lessons were delivered; brief teacher reflection (what worked / challenges) collected via short form or log. | |
| **5** | __ / __ / __ – __ / __ / __ | Deliver further Module 3 lesson(s); introduce simple project or mini-task for students (e.g. small awareness activity). | Use Platform Resources and Links to support student tasks; if possible, create or join a national Discussion group to compare ideas between classes/schools. | Record number of classes/students taking part in the mini-task; note whether at least one national Discussion group is active; simple qualitative notes on type of exchanges. | |
| **6** | __ / __ / __ – __ / __ / __ | Deliver Module 4 (e.g. social / ethical aspects, rights, responsibilities) and link to real-life cases; run a classroom discussion or debate. | Use Module 4 on Platform; prepare 2–3 guiding questions and post them in class or national Discussions for asynchronous continuation of the debate. | Document which classes completed Module 4; count number of Discussion threads and replies; collect short student feedback (1–2 questions) or exit tickets if feasible. | |

| | | | | | |
|---|---|---|---|---|---|
| **7** | __ / __ / __ – __ / __ / __ | Deliver Module 5 (e.g. cyberpeace / democracy / resilience) and organise a class reflection on what students have learned across modules. | Use Module 5 and key Resources; ask students to post one "most important learning" in the Discussion room; optionally open or join a cross-country Discussion group. | Record completion of the full module sequence in each piloting class (or note partial completion); count number of schools/classes involved in cross-country Discussions; note number of posts. | |
| **8** | __ / __ / __ – __ / __ / __ | Run at least one career and study pathways activity using the Guides (e.g. "Find your cyber profile" or mapping study paths); encourage students to think about next steps. | Use Guides and any supporting materials (career profiles, study pathways); invite questions for a future Q&A with a cybersecurity professional via the Discussions section. | Count number of classes using the Guides; collect simple stats on how many students completed the activity; optional short student poll about interest in cybersecurity careers. | |
| **9** | __ / __ / __ – __ / __ / __ | Prepare or run a student-led mini-project (poster, campaign, short presentation, peer awareness session); classes finalise outputs. | Use Platform to share project ideas or drafts (via Discussions, if appropriate); encourage students to post one photo/description of their project in a national or cross-country Discussion group. | Document number and type of mini-projects completed; approximate number of students involved; note engagement in Discussions related to projects (posts/comments). | |
| **10** | __ / __ / __ – __ / __ / __ | Organise a sharing event at school level (internal showcase, small fair, or online session) where students present key outcomes and takeaways. | Use Platform to host an asynchronous reflection thread on the event ("What did we learn?"); if feasible, invite a guest cybersecurity professional to comment or respond in Discussions. | Collect short teacher/student feedback on the event; record whether a guest professional took part (yes/no, how many); note level of participation in the related Discussion thread. | |
| **11** | __ / __ / __ – __ / __ / __ | Conduct wrap-up lessons: revisit main concepts, answer remaining questions, discuss how to apply learning in everyday life; clarify any pending tasks. | Use Modules/Resources selectively for review; encourage final posts in class or cross-country Discussions (e.g. "one commitment I will keep online"). | Apply post-test / end-line questionnaire (if used); summarise which modules and activities each class completed; teachers update simple KPI dashboard (per class/school). | |



Co-funded by the European Union

| | | | | | |
|---|---|---|---|---|---|
| **12** | __ / __ / __ – __ / __ / __ | Final reflection and closure of piloting at school level; teachers compile evidence and prepare school report for national partner. | Platform use mainly for closing messages, final reflections, or showcasing best student posts/projects in Discussions; ensure all necessary data are downloaded or noted. | Consolidate all data for the school (numbers of teachers, students, modules delivered, Guides used, Discussion groups/posts, events, professionals involved); submit school-level KPI and reporting templates by agreed deadline. | School sends report & data |

*Table C1: Piloting activities.*

**Summary**

**Piloting weeks used:** _____

**Modules delivered (tick):** ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

**Career & pathways activities (Guides used):** Yes / No – note: _____

**Cross-country Discussions:** Yes / No – note: _____

**Buffer for nat. aggregation/reporting:** from ___ / ___ / 20__ to ___ / ___ / 20__

**Guidance for Completing the EnCycLEd National Piloting Calendar**

1. **Fill in the header section**

○ Indicate your **country, partner organisation, academic year/term**, and the **piloting window at school level**.

○ Set the **school report deadline** to the national partner and the **national report deadline** to the consortium, keeping in mind that **all piloting activities and deliverables must be completed before 30 November 2026**, with piloting ending **1–2 months earlier**.



Co-funded by the European Union

2. **Map "Weeks 1–12" to real dates**

○ For each week, replace __ / __ / __ – __ / __ / __ with concrete calendar dates, using your **national school calendar** and the common **EnCycLEd Gantt**.

○ The suggested activities in the table (under "Main piloting activities", "Platform use" and "Data & KPIs") are an example sequence. You may adapt the pacing, combine weeks, or extend them, provided you respect the project end date and reporting needs.

3. **Flexibility in number of modules**

○ Please indicate clearly which modules you plan to deliver, so that the consortium can interpret KPIs correctly.

○ Please indicate clearly in the "Main piloting activities" and "Summary" which modules and activities you actually plan to deliver, so that the consortium can interpret KPIs correctly.

4. **Use the "Data & KPIs" and "Notes/reporting" columns**

○ Briefly describe what information will be collected each week (e.g. number of classes/students, modules completed, use of Discussions, feedback tools).

○ Use the "Notes/reporting" column to indicate any special events, cross-country activities, or issues to be flagged.

Once completed, please share your national piloting calendar with the project coordinator by the agreed deadline. This will help ensure that all piloting activities are realistic, comparable and aligned with the overall EnCycLEd timeline and KPIs.

# ANNEX D

## Minimum Piloting Package and Piloting-related KPIs per Partner

### 1. Purpose of this Annex

This Annex sets out the minimum expectations for piloting in each school and the quantitative minimum targets for piloting-related KPIs across all partners. It translates the project proposal, the logical framework and the Piloting Deliverables Distribution Excel sheet into a single operational reference so that every partner knows:

- what their minimum contribution is (modules, activities, numbers of students/teachers, cross-country exchanges);
- how these contributions map to the Key Performance Indicators (KPIs); and
- how results will be monitored and aggregated under Work Package 4 (WP4).

UACS, as leader of WP4 ("Implementation and Piloting / lessons learned / cross-cutting Evaluation and Sustainability Assessment"), is responsible for maintaining this Annex, updating it if needed (with partner agreement), and using it as a basis for Monitoring, Evaluation and Learning (MEL).

### 2. Minimum piloting package per school (Options A, B, C)

To keep piloting manageable and still fulfil the proposal commitments, each piloting school is expected to implement at least one minimum piloting package. Three options are defined:

- **Option A – Full package (default for main piloting schools)**
  - Modules: all 5 EnCycLEd modules (Modules 1–5) delivered to at least one coherent cohort.



Co-funded by the European Union

○ Guides: at least 1 structured activity using the Cybersecurity Careers and Study Pathways Guides.

○ Students: at least 50–60 students directly involved in the full set of piloted modules.

○ Platform registrations: reach the school's registration minima (AFS 250, SU 200, KVS 250 students) as specified in this Annex.

○ Discussions: at least 3 purposeful uses of the Discussions section (e.g. reflection thread, cross-country Discussion, Q&A with a professional).

○ Cross-country: participation in at least 1 cross-country team/activity.

**● Option B – Core package**

○ Modules: at least 3 modules, including Module 1, one technical module (2, 3 or 4) and Module 5 (Cyberpeace).

○ Guides: at least 1 structured Guides activity.

○ Students: at least 30–40 students involved in the piloted modules.

○ Platform registrations: still aim towards the same registration minima, concentrating on one or two classes.

○ Discussions: at least 2 purposeful uses of Discussions (e.g. reflection + cross-country/Q&A).

○ Cross-country: participation in at least 1 cross-country Discussion-based activity.

**● Option C – Light package**

○ Modules: at least 1 module (preferably Module 1 or a technical module).

○ Guides: at least 1 Guides-based activity.

- Students: at least 20–30 students involved.
- Discussions: at least 1 use of Discussions (reflection or Q&A).

Option C is intended only for exceptional cases (e.g. late entry, small additional schools) and may be used only with prior agreement from WP4 (UACS) and the national piloting coordinator. Its use must not jeopardise the consortium's ability to reach the overall KPI minima presented in this Annex (students reached, modules delivered, cross-country activities, platform use).

The detailed numeric minima per school and partner below assume that the main piloting schools (AFS, SU, KVS) will normally implement Option A or B, with Option C reserved for special circumstances.

The minimum student numbers in Options A/B/C refer to students who participate in the piloted modules, not to the total numbers of students registered on the Platform or informed about it (these are specified separately in the KPI tables).

**3. Partner roles and KPI levels**

For the KPIs in this Annex, we use the following shorthand:

- Piloting schools: AFS, SU, KVS
- HEIs (non-school pilot partners): UIBK, HU, UoM
- Non-school partners: AC (platform & training), REACH (dissemination & sustainability)
- WP4 lead: UACS (MEL coordination and aggregation – no numeric minimums as such, but responsible for ensuring totals match proposal commitments)

KPI level key:

- S = school-level KPI (each piloting school reports)
- C = country-level KPI (piloting partner aggregates)



Co-funded by the European Union

● P = project-level KPI (WP4/UACS and other WPs consolidate and report)

## 4. Piloting-related KPIs – narrative overview of minimum targets

Below is a short narrative explanation of the KPIs; the full numeric distribution per partner is provided in the table that follows.

K1 – Teachers and students involved in piloting (Level: S / C)

Each piloting school should involve at least 60 participants (teachers + students) at AFS, 50 at SU and 50 at KVS. UACS aggregates these figures to check that the consortium meets overall participation targets.

K2 – Teachers/future teachers registered on the Platform (Level: S / C / P)

Each piloting school registers 33 teachers/future teachers (≈100 across AFS, SU, KVS). UACS verifies totals vs proposal; the platform provider supplies registration statistics.

K3 – Students registered on the Platform (Level: S / C / P)

Piloting schools register 250 (AFS), 200 (SU) and 250 (KVS) students; HEIs register 100 students each (UIBK, HU, UoM). The project-level total is 1 000 students registered. AC ensures registration and reporting; UACS aggregates.

K4 – Other teachers informed about the Platform (Level: C / P)

Piloting schools inform 50 additional teachers each; UIBK and HU each inform 20, UoM 3, AC 3 and REACH 3. UACS aggregates and checks this against outreach commitments.

K5 – Students informed about the Platform (Level: C / P)

AFS, SU, KVS inform 500 / 400 / 500 students respectively; UIBK, HU, UoM each inform 200 students. The project-level total is 2 000 students informed, used for wider reach and dissemination.

K6 – Cross-country teams on the Platform (Level: P)

At project level, at least 20 cross-country teams are formed (10 school-based teams and 10 developer/teacher teams involving AFS, SU, KVS, HU, UIBK). Each piloting school and HEI should appear in at least one teacher team and one student/developer team.

K7 – Cross-country learning/exchange sessions (Level: P)

At least 10 cross-country learning/exchange sessions (or equivalent Discussion-based activities) are hosted on the platform. Each session should include ≥2 interactions from different countries. Schools/HEIs contribute at least one such activity per country; AC provides logs; UACS uses this KPI for cross-learning (D4.5).

K8 – Platform Discussions KPIs (D1–D7) (Levels: S / C / P)

From K2–K7 and platform statistics, UACS and AC derive:

- D1: teachers using Discussions – all piloting teachers expected to use it at least once;
- D2: at least 20 Discussion Groups (one per cross-country team plus class groups);
- D3: at least 20 cross-country Discussion Groups;
- D4: a substantial share of registered students participate in at least one group;
- D5: each country involves at least one guest professional (overall ≥ 5–9);
- D6: minimum 20 cross-country interactions (2 per session) with a higher aspirational target;
- D7: qualitative descriptions of the types of exchanges.

## 5. How to read the KPI–partner table

The table that follows this introduction provides a row-by-row breakdown of:

- each KPI (K1–K7, D1–D7),
- its level (S, C or P),
- and the minimum numeric contribution expected from each piloting school and HEI.

The notes column explains how each KPI relates to WP4 monitoring, platform statistics and dissemination work. Partners are expected to use this Annex, together with the minimum piloting package (Options A/B/C) and the National Piloting Calendars, as their shared reference when planning, implementing and reporting on piloting.

| KPI_ID | Level | KPI Description | Unit | Piloting AFS_Min | Piloting SU_Min | Piloting KVS_Min | UIBK_Min | HU_Min | UoM_Min | Project_Total_Target | Notes_Level_and_Responsibility |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **K1** | S/C | Number of teachers and students involved in piloting (direct participants) | # persons | 60 | 50 | 50 | | | | | School + country totals must meet proposal targets; reported by schools, aggregated by country, checked by WP4/UACS |
| **K2** | S/C/P | Number of teachers (and future teachers) registered on the Platform | # teachers | 33 | 33 | 33 | 0 | 0 | 0 | ≈100 | School-level registration; WP4/UACS verifies total vs logframe; platform provider supplies stats |
| **K3** | S/C/P | Number of students registered on the Platform | # students | 250 | 200 | 250 | 100 | 100 | 100 | 1000 | All piloting schools and HEIs register the indicated minimum; platform provider supplies stats; WP4 aggregates |
| **K4** | C/P | Number of other teachers / future teachers informed about the Platform (non-registered) | # teachers informed | 50 | 50 | 50 | 20 | 20 | 3 | 199 | Reported by each partner; WP4 aggregates to check outreach KPI |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **K5** | C/P | Number of students informed about the Platform (beyond those registered) | # students informed | 500 | 400 | 500 | 200 | 200 | 200 | 2000 | Reported by each partner; WP4 aggregates; also used in dissemination/sustainability messages |
| **K6** | P | Number of cross-country teams (teachers or students) formed and interacting on the Platform | # teams | | | | | | | 20 | Composed of school-based teams (AFS, SU, KVS) and developer/teacher teams (AFS, SU, KVS, HU, UIBK); coordinated by WP4 |
| **K7** | P | Number of cross-country learning and exchange sessions hosted on the Platform | # sessions | | | | | | | 10 | Each session must include ≥2 interactions from different countries; schools/HEIs participate; WP4 interprets for D4.5 |
| **D1** | S/C/P | Teachers using Discussions section | # teachers using Discussions | ≥ all piloting teachers registered and delivering modules | ≥ all piloting teachers registered and delivering modules | ≥ all piloting teachers registered and delivering modules | | | | [derived from K2 and activity logs] | Each piloting teacher should use Discussions at least once; platform provider supplies usage stats; WP4 aggregates |



Co-funded by the European Union

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **D2** | P | Discussion Groups created | # Discussion Groups | | | | | | | ≥20 | At least one group per cross-country team plus additional class groups; exact per-partner distribution defined in National Piloting Calendars |
| **D3** | P | Cross-country Discussion Groups | # cross-country Groups | | | | | | | ≥20 | All 20 cross-country teams (K6) should correspond to at least one cross-country Discussion Group; platform stats used; WP4 aggregates |
| **D4** | S/C/P | Students registered in Discussion Groups | # students in Discussions | [subset of 250] | [subset of 200] | [subset of 250] | [subset of 100] | [subset of 100] | [subset of 100] | [derived from K3] | Subsets of registered students participate in at least one Discussion Group; exact numbers per country defined in MEL toolkit |
| **D5** | P | Guest cybersecurity professionals / role models participating in Discussions | # guest professionals | | | | | | | ≥5–9 | Each country strongly encouraged to involve ≥1 professional; final numeric target and distribution agreed at Malta; WP4 tracks |
| **D6** | P | Interactions in Discussion Groups (posts, replies, comments) | # interactions (approximate) | | | | | | | ≥20 cross-country interactions minimum | Per Excel definition: ≥2 interactions from different countries per cross-country team/session (K7); aspirational target may |



Co-funded by the European Union

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | be higher; platform logs used |
| **D7** | C/P | Qualitative description of types of exchanges in Discussions | Text | Qualitative summary per school/country | Qualitative summary per school/country | Qualitative summary per school/country | Qualitative summary per country | Qualitative summary per country | Qualitative summary per country | N/A | Partners describe main types of exchanges (reflection, Q&A, group work, cross-country debate, campaign planning); WP4 synthesises |