CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

R5. Policy Recommendation Paper on Data security and Cyber security, specifically tailored for schools, following the ISO 27001, 27002, 27701, 22301 and 31000 standards

Conscious Youth Behaviours in Emerging Realities

Lead partner: SIGMA BUSINESS NETWORK, Greece

Co-funded by the European Union

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

Document Information

Grant Agreement #	**2023-1-EL01-KA220-SCH-000156982**
Acronym	**C.Y.B.E.R.**
Title	**Conscious Youth Behaviours in emerging realities**
Start Date:	16/11/2023
Result:	Policy Recommendation Paper R5
Related Activities:	A4.5 - Design and development of R5
Lead Organisation:	SIGMA Tournis Symvouleftiki EE, Greece
Contributing Partners:	• PRISM IMPRESA SOCIALE S.R.L. , Italy • County Centre for Educational Resources and Assistance Botoșani, Romania • CPM-Centrum Prevencie Mladeze, Slovakia • Casa Do Professor, Portugal • Vitale Tecnologie Comunicazione - VITECO SRL, Italy • EUROCERT Eyropaiki Etaireia Emeghon Kai Pistopoihseon Anonymos Etaireia, Greece
Dissemination Level	Public
Disclaimer	The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Document History

Date	Submitted by	Reviewed by	Version (Notes)
26/06/2026	SIGMA	Theodora Ntinou	1.0

About CYBER	
Action type	Erasmus+ KA220-SCH - Cooperation partnerships in school education
Priority	SCHOOL EDUCATION: Development of key competences ▪ Addressing digital transformation through development of digital readiness, resilience and capacity ▪ Inclusion and diversity in all fields of education, training, youth and sport

The project aims to address a crucial question: How does cyberspace influence human behaviour, particularly among young people? In today's digital age, online behaviour has become deeply embedded in the psychological environment of cyberspace. It offers unique opportunities for shaping human interaction but also raises concerns due to its borderless nature. While the internet brings undeniable social and economic benefits, it has challenged core European values such as equality, human rights, and democracy. To build a safer internet, a collective effort is essential. Sharing best practices and educating young generations, teachers, and parents are pivotal steps toward fostering a safer online environment.

CYBER strives to develop the cyber resilience of European schools by creating tailored EU quality procedures for the school system, and by equipping the professors and students with the tools and knowledge to discuss conscious and unconscious online behaviours of adolescents, cyberpsychology and the downsides of the Internet overuse, to enhance the classrooms understanding of the dangerous emerging behaviours a young user may incur.

CYBER is going to structure a methodology to integrate the crucial topics of cyberthreats and cyberpsychology within the classroom and the school system, fostering dialogue among students on the dangerous emerging behaviours towards themselves and their peers. In addition, the project sets clear procedures on cyber and data protection to have schools obtain the CYBER certification, requirements for establishing, implementing, maintaining and improving information security management at school.

The project results are meant to benefit every adolescent in every European country, especially those who were born in the digital era. The social context in these matters (hacking of profiles, fake news, fake identities, online fraud/scam, online blackmailing, revenge porn, hikikomori, cyberbullying, etc.) holds a stronger value, where the education and awareness of young people on the problem have a way greater impact than a national rule.

Table of Contents

Introduction

This document is the Cyber Resilience Policy for Schools, developed as part of the C.Y.B.E.R. (Conscious Youth Behaviours in Emerging Realities) project. The project is co-funded by the European Union under the Erasmus+ Programme and brings together partner organisations from Greece, Italy, Portugal, Romania, and Slovakia.

Schools today rely heavily on digital technology. Students use online platforms to learn, teachers communicate through digital tools, and staff manage records in connected systems. This is a positive development, but it also means that schools face risks they did not face before: cyberattacks, data breaches, cyberbullying, and the impact of digital life on students' mental health.

This policy is designed to help every school in the five partner countries deal with these challenges in a practical way. It brings together European law, the national rules of each country, internationally recognised security standards, and the best available research, all in one document that any school can read and use.

This is not a technical manual. It is a guide for everyone who works in a school: the principal, teachers, administrative staff, and IT coordinators. You do not need a legal or technical background to use it. The policy explains what the law requires, what good practice looks like, and what your school needs to do.

The templates and tools provided in the appendices are designed as adaptable starting points. Schools are encouraged to modify them to suit their national legal context, internal procedures, and specific circumstances.

Who This Policy Is For

This policy is for everyone involved in running a school: the principal, deputy principal, teachers, IT coordinators, administrative school staff, and school boards. It is written to be understood by anyone, regardless of their background.

How This Document Is Organised

Part	Content
Part 1: The Legal Framework	What European law says schools must do, explained in plain language.
Part 2: Your Country's Rules	The specific national rules that apply in each of the five countries.
International Standards and Schools	How five internationally recognised management standards shape the practical recommendations in this policy.
Part 3: What Your School Should Do	Practical steps organised by topic, based on international standards and EU law.
Part 4: What the Evidence Shows	What scientific research tells us about what actually works in schools.

Part	Content
Appendixes	Template documents and practical implementation tools for schools to adapt and use directly.
References	The national legislative instruments and official sources used in the preparation of Part 2.

Part 1: The Legal Framework

Schools in all five partner countries must follow European laws that govern how they handle data and protect students online. This part explains what those laws require, in plain language. There are six main legal instruments that every school needs to know about. Together they cover data protection, cybersecurity, artificial intelligence, online platforms, digital communications, and the security of digital products.

1.1 General Data Protection Regulation (GDPR)

GDPR is the foundation of data protection in Europe. It applies to every organisation that handles personal data, and that includes schools. In a school, personal data includes student names and identification numbers, attendance records, grades, health information, photos, and any other information that relates to an identifiable person.

GDPR recognises children as a particularly vulnerable group. Schools must therefore apply a higher standard of care when handling student data than they would for adults.

What the GDPR requires from schools:

- Schools should have a clear legal basis for every data processing activity. In most cases this will be a legal obligation required by national education law, a public task necessary for running the school, or in some cases consent.
- Schools should only collect the data they actually need. They must not collect additional information simply because it might be useful one day.
- Schools should appoint a Data Protection Officer (DPO). Depending on the country, this may be managed at authority or cluster level rather than for each individual school.
- Schools should carry out a Data Protection Impact Assessment (DPIA) before introducing any new digital system that involves large-scale processing of student data or behavioural monitoring. A template is included in Appendix V.
- Schools should report personal data breaches to the national supervisory authority within 72 hours of becoming aware of them.
- Schools should inform students and parents about how their data is used, in clear and plain language.
- Students and parents have the right to access the data held about them, to request corrections, and in some circumstances to request deletion.

Age of Digital Consent

The GDPR allows each EU country to set the age at which a young person can consent to using digital platforms without parental approval. This age ranges from 13 to 16 years across the five partner countries. For students below the national age of digital consent, schools must obtain written parental or guardian consent before enrolling them on digital platforms. The specific age for each country is set out in Part 2.

1.2 NIS2 Directive

NIS2 Directive sets out a common European framework for cybersecurity. It requires organisations to have adequate cybersecurity measures in place, to manage the risks posed by their digital suppliers, and to report significant cybersecurity incidents to the national authority.

Schools are not always directly classified as essential or important entities under NIS2. However, schools depend heavily on digital systems, and cybersecurity incidents affecting those systems can disrupt education and put student data at risk. The NIS2 framework sets the standard that all schools should aim for, regardless of whether they are formally classified.

What NIS2 means for schools:

- Schools should implement cybersecurity measures that match the risks they face. At a minimum this means strong passwords, regular backups, and protected networks.
- Schools should check the cybersecurity practices of their digital suppliers. A platform used for student records must be as secure as the school itself.
- Schools should have a procedure for detecting and responding to cybersecurity incidents. Staff must know who to contact and what steps to follow.
- Schools should provide regular cybersecurity awareness training for all staff.
- Significant incidents should be reported to the national cybersecurity authority. Deadlines and authorities differ by country. See Part 2.

1.3 EU Artificial Intelligence Act

AI Act is the first comprehensive European law governing the use of artificial intelligence. It came into force in August 2024 and applies progressively until full implementation in August 2026. Schools increasingly use AI-supported tools: adaptive learning platforms, automated grading systems, chatbots, and learning analytics. AI Act creates clear rules for how these tools can and cannot be used.

What AI Act requires from schools:

- Certain AI uses in schools are completely prohibited. These include emotion recognition systems used to monitor students, biometric categorisation of students, and real-time facial recognition in educational settings. There are no exceptions for schools.
- AI systems used for student assessment, admissions, or monitoring are classified as high-risk and must meet strict requirements for transparency, human oversight, and documentation.
- Students and parents should be informed when AI tools are used in ways that affect educational decisions.
- A teacher should always review and take responsibility for any AI-generated recommendation that affects a student. AI cannot make final decisions about students.

- Schools should maintain a written list of all AI tools in use, including what each tool does and what data it processes.

1.4 Digital Services Act (DSA)

DSA regulates online platforms and digital services. It requires platforms to be more transparent, to provide accessible ways to report harmful content, and to strengthen protections for young people. Schools have an important role in helping students understand how online platforms work and how to protect themselves.

What DSA means for schools:

- Schools should teach students how to recognise and report harmful content on the platforms they use.
- Schools should help students understand how recommendation algorithms work and how they shape what young people see online.
- Teachers should be aware of the obligations that the DSA places on major platforms and be able to discuss them with students as part of digital literacy education.

1.5 ePrivacy Directive

ePrivacy Directive protects the confidentiality of electronic communications. It applies to email systems, messaging platforms, video conferencing tools, and any other digital communication service used in schools.

What ePrivacy Directive means for schools:

- Digital communications between students, parents, teachers, and administrative staff should be secure and confidential.
- Video conferencing tools used for remote learning should be configured to prevent unauthorised access. Virtual classrooms should require a login before anyone can join.
- Lessons and meetings should not be recorded without the explicit consent of all participants.
- School websites and platforms that use cookies should display a compliant cookie notice.

1.6 Cybersecurity Act

Cybersecurity Act strengthens the role of ENISA, the EU Agency for Cybersecurity, and establishes a European framework for certifying digital products and services as secure. It supports the adoption of trustworthy technologies across the EU, including in schools.

What Cybersecurity Act means for schools:

- When schools choose digital tools, platforms, or equipment, they should take cybersecurity into account and prefer certified or approved products where possible.
- Connected classroom devices such as smart boards, tablets, and cameras should be securely configured and kept up to date.
- Schools can consult ENISA guidance and tools to help plan their cybersecurity approach.

1.7 How These Laws Work Together

These six legal instruments are not separate obligations to be addressed one by one. They form an integrated framework. A school that protects student data under the GDPR, manages cybersecurity under NIS2, uses AI responsibly under the AI Act, teaches digital literacy in line with the DSA, secures its communications under the ePrivacy Directive, and selects trusted technologies in line with the Cybersecurity Act will have addressed the full range of its legal obligations.

Law	The key obligation for schools
GDPR	Protect personal data, appoint a DPO, get consent where needed, report breaches within 72 hours.
NIS2 Directive	Have cybersecurity measures in place, check your suppliers, report incidents, train your staff.
EU AI Act	Do not use prohibited AI, keep humans in charge of decisions, inform students and parents.
Digital Services Act	Teach students to report harmful content and understand how algorithms work.
ePrivacy Directive	Secure digital communications, protect virtual classrooms, follow cookie rules.
Cybersecurity Act	Consider security when buying technology, secure connected devices, use ENISA guidance.

Part 2: What Applies in Your Country

European law sets the common framework, but each country also has its own national laws and guidance that schools must follow. This part summarises the most important national rules for each of the five partner countries. Find your country and check what applies to you.

2.1 Greece

Greece operates a highly centralised model for school digital governance. Cybersecurity, data protection, and digital infrastructure are managed primarily at national level by the Ministry of Education and the Ministry of Digital Governance. Individual schools function mainly as users of centrally managed systems, including the MySchool student information system, the e-Class learning platform, and the Panhellenic School Network (PSN).

Area	What It Means for Schools
NIS2 Transposition Law 5160/2024	• Schools must implement risk management measures and ensure that third-party digital platforms (e.g. Webex) comply with cybersecurity standards.

Area	What It Means for Schools
MD 1689/2025 MD 1899/2025	• Mandatory incident reporting: schools must notify EAKE of significant cybersecurity incidents. • Formal security policies are required covering access control to student data, backup procedures, encryption of communications, and supply chain security for software and hardware used in schools. • Staff training and cyber hygiene are required: school personnel are frequent targets of phishing and social engineering attacks. • Schools must maintain documentation including security policies, training records, network diagrams, and periodic security audit results. • MD 1899/2025 requires designation of a cybersecurity responsible role and formal incident response and escalation procedures.
Data Protection Law 4624/2019	• Governs the processing of personal data by public sector bodies including schools, in line with GDPR principles. • Establishes the role and supervisory powers of the Hellenic Data Protection Authority (HDPA). • DPO responsibilities are managed at authority level rather than for each individual school. • Schools must notify the HDPA (Hellenic Data Protection Authority) within 72 hours of any personal data breach likely to create a risk to individuals. • Schools must implement appropriate security measures for student, parent, and staff data.
Age of Digital Consent	• 15 years. • Schools must obtain written parental or guardian consent before enrolling students under 15 on any digital platform that processes their personal data.
Cyberbullying Law 5029/2023	• Provides a structured legal framework for the prevention and management of cyberbullying in schools. • Introduces the national reporting platform stop-bullying.gov.gr for the formal submission and tracking of incidents. • Schools must actively participate in the identification, reporting, and management of cyberbullying cases. • Schools must have a written procedure for responding to cyberbullying incidents.
Mobile Phones	• Students are prohibited from possessing or using mobile phones on school premises. • Zero-tolerance policy in place since 2024. • Violations result in immediate disciplinary consequences including suspension.

Area	What It Means for Schools
AI in Education	• No specific national guidelines have been issued for AI use in schools. • The EU AI Act applies directly. • Schools should exercise caution when using AI tools that process student data.
Digital Infrastructure	• MySchool: national student information system, centrally managed. • e-Class: national learning management platform. • Panhellenic School Network (PSN): secure national connectivity infrastructure for all public schools.
Key Contacts	• Cybersecurity: EAKE (cyber.gov.gr) • Data Protection: HDPA (dpa.gr) • Cyberbullying: stop-bullying.gov.gr

2.2 Italy

Italy operates a predominantly centralised model, although schools retain a degree of organisational autonomy. The National Cybersecurity Agency (ACN) plays a central role in coordination and incident management. Schools depend heavily on ministerial guidance and centrally managed platforms, including the Unica national platform. The Garante has issued school-specific guidance and FAQs that schools should consult alongside the GDPR.

Area	What It Means for Schools
NIS2 Transposition Legislative Decree 138/2024 Law 109/2021	• Legislative Decree 138/2024 shapes expectations on risk assessment, supplier security, and incident reporting even for schools not directly classified as NIS entities. • Schools must govern third-party ICT services and maintain structured reporting channels when incidents affect educational activities or student data. • Law 109/2021 establishes the National Cybersecurity Agency (ACN), which plays a central coordination role for cybersecurity governance across public institutions including schools.
Data Protection Legislative Decree 196/2003 (as amended by Decree 101/2018)	• Governs the processing of students', parents', teachers', and staff data within school activities. • The supervisory authority is the Garante per la protezione dei dati personali. • DPO designation is mandatory for public schools but may be organised at school level or through shared arrangements across multiple schools. • Parental authorisation is required for processing children's data where digital services are offered directly to students below the age of digital consent.

Area	What It Means for Schools
	• Schools must inform students and parents of their data rights and manage data breaches in line with GDPR requirements.
Age of Digital Consent	• 14 years. • Parental consent is required for students under 14 for enrolment on learning management systems, publication of photographs, and any processing involving minors in an educational setting.
Cyberbullying Law 71/2017	• Provides a legal framework for combating cyberbullying in schools. • Schools must have written procedures for handling incidents and supporting victims. • Schools may request the removal of harmful content from online platforms.
Mobile Phones MIM Note 5274/2024 MIM Circular 3392/2025	• Smartphones are restricted during all school activities across all educational cycles. • The restrictions aim to protect the educational environment and promote age-appropriate use of digital tools. • Limited exceptions apply for specific educational activities or accessibility needs.
AI in Education Ministerial Decree 166/2025	• National guidelines require transparency about AI use in schools. • Human oversight of AI-supported educational decisions is mandatory. • AI tools that process student data must comply with GDPR requirements.
Digital Platforms	• Unica: national platform for administrative and educational functions. • Microsoft 365 for Education: institutionally managed suite for teaching and communication. • Digital Integrated Teaching (DDI) framework (MD 89/2020) requires schools to regulate the use of digital platforms, student access, and teacher responsibilities in online educational environments.
Key Contacts	• Cybersecurity: ACN (acn.gov.it) • Data Protection: Garante (garanteprivacy.it)

2.3 Portugal

Portugal has one of the most structured national frameworks for school digital governance among the five countries. Schools benefit from the mandatory PADDE (School Digital Development Action Plan), the SeguraNet support programme, and CERT.PT for incident response. NIS2 Directive was transposed through Decree-Law 125/2025, which came into force on 3 April 2026.

Area	What It Means for Schools
NIS2 Transposition Decree-Law 125/2025 (in force 3 April 2026) Law 46/2018	• Schools qualifying as Relevant Public Entities (Group A or B) must implement cybersecurity risk management measures. • Mandatory designation of a cybersecurity responsible officer. • Significant incidents must be reported to the CNCS within 24 hours. • Schools must identify critical digital assets, establish incident response procedures, and ensure continuity of operations. • Law 46/2018 remains the foundational framework establishing the CNCS as the national cybersecurity authority.
Data Protection Law 58/2019	• A DPO is mandatory at the level of each school cluster (agrupamento de escolas), not individual schools. • The DPO must be registered with the CNPD (Comissão Nacional de Proteção de Dados) and is responsible for monitoring GDPR compliance, advising staff, conducting training, and liaising with the CNPD. • Schools must notify the CNPD within 72 hours of a personal data breach likely to result in a risk to individuals. • Schools must maintain a register of processing activities and implement appropriate security measures.
Age of Digital Consent	• 13 years. This is the lowest threshold among the five countries. • Verifiable parental or guardian consent is required before enrolling students under 13 on any digital platform or online tool that processes personal data. • This applies to learning management systems, publication of photographs, and any processing involving minors.
Cyberbullying SeguraNet Programme	• SeguraNet (managed by DGE in partnership with CNCS) provides specific guidance on cyberbullying prevention and response. • Schools must integrate cyberbullying prevention into their PADDE and internal regulations. • Template incident response procedures and Acceptable Use Policy documents are available through SeguraNet.
Mobile Phones Decree-Law 95/2025 (in force September 2025)	• Smartphones are legally prohibited for all students in years 1 to 6 in all public and private schools. • For cycles 3 and secondary, the Ministry has issued recommendations encouraging restrictions, with schools retaining autonomy to formalise rules in their internal regulations. • Any recording of students requires explicit consent under GDPR.

Area	What It Means for Schools
Mandatory School Digital Plan PADDE Framework	• Every school cluster must develop and maintain a PADDE (School Digital Development Action Plan). • The PADDE must explicitly include cybersecurity measures and covers three dimensions: organisational (leadership and governance), pedagogical (digital citizenship and safe internet education), and technological (infrastructure and security). • Schools must adopt an Acceptable Use Policy and establish incident response procedures with reference to CERT.PT.
AI in Education	• No specific national guidelines have been issued yet. • EU AI Act applies directly. • The DGE has acknowledged the need for a national framework and is expected to issue recommendations. • Schools should exercise caution when using AI tools that process student data.
Digital Infrastructure	• RCTS (managed by FCCN): national high-speed secure network for all public school clusters. • Microsoft 365 for Education: nationally managed suite for teaching and communication. • CERT.PT (operated by CNCS): national CSIRT and incident response contact for the education sector.
Key Contacts	• Cybersecurity: CNCS (cncs.gov.pt) • Incident Response: CERT.PT • Data Protection: CNPD (cnpd.pt) • Digital Safety: SeguraNet (seguranet.pt)

2.4 Romania

The national framework is coordinated by the Ministry of Education in collaboration with the National Cyber Security Directorate (DNSC), within the broader national and European cybersecurity policy framework. In many schools, cybersecurity-related responsibilities are assumed by the school principal, ICT coordinator, or a designated teacher, as dedicated cybersecurity staff are uncommon. Romania faces some of the largest implementation gaps among the five partner countries, but there is growing momentum to address them.

Area	What It Means for Schools
NIS2 Transposition OUG 155/2024 (approved by Law 124/2025) Law 58/2023	• OUG 155/2024 applies directly to higher education. For pre-university schools, applicability is not fully clear but schools interacting with government networks (e.g. SIIIR) are expected to follow NIS2 protocols. • Schools are expected to report significant incidents to the DNSC within 24 hours via the PNRISC platform. • Required measures include: network segmentation (separate Wi-Fi for administration and students), multi-factor

Area	What It Means for Schools
	authentication for access to official platforms, risk analysis policies, and mandatory cyber hygiene training for all staff. • Supply chain security: private vendors of e-learning platforms or accounting software used by schools must be NIS2-compliant. • Law 58/2023 establishes that responsibility for cybersecurity lies with the entity that owns or manages the network, making school management directly accountable.
Data Protection Law 190/2018	• Schools are classified as independent data controllers and must ensure full GDPR compliance. • A shared DPO arrangement is permitted at county inspectorate or central level. • Schools must implement mandatory parental consent procedures for online learning platforms and for the use of students' images. • Video surveillance is permitted only for protection of persons and property, with mandatory notification of students, teachers, and visitors. Recordings must not be kept for more than 30 days except for investigated incidents. • Exam results must be published using anonymisation or pseudonymisation in line with ANSPDCP guidelines.
Age of Digital Consent	• 16 years. This is the highest threshold among the five countries. • Parental or guardian consent is required before enrolling students under 16 on any digital platform. • In practice, this applies to virtually all digital educational tools used in Romanian schools.
Cyberbullying ROFUIP 2025/2026 Student Statute (Order 5707/2024)	• ROFUIP defines and penalises cyberbullying as a prohibited behaviour within the school environment. • Unauthorised video or audio recording of teaching activities is prohibited. • Staff should use only officially approved digital tools and treat student data with strict confidentiality. • Student Statute explicitly prohibits any form of aggression in the virtual environment. • No dedicated national reporting platform exists. Incidents are handled through the school and referred to the ANSPDCP where personal data is involved.
Mobile Phones Law 198/2023 ROFUIP	• Mobile phone use during lessons is prohibited for preschool, primary, and lower secondary students, except when authorised by the teacher for educational purposes. • Phones must be switched off or on silent mode during classes and stored in a designated location per ROFUIP. • Rules for phone use during breaks are set by each school's own Internal Regulations.

Area	What It Means for Schools
AI in Education	• No specific national guidelines have been issued. The EU AI Act applies directly. • The Ministry of Education has not issued guidance on generative AI tools such as ChatGPT, creating a significant gap. • Schools should apply the AI Act's requirements on transparency, human oversight, and data protection when using any AI tool with students.
Digital Infrastructure	• No unified national school network exists. Schools rely on commercial internet providers, leading to non-uniform cybersecurity standards. • SIIIR (centrally managed by the Ministry) is the main national database for student data. • Schools use commercial platforms (Google Workspace, Microsoft 365) under individual contracts.
Key Contacts	• Cybersecurity: DNSC (dnsc.ro) • Data Protection: ANSPDCP (dataprotection.ro)

2.5 Slovakia

Slovakia has demonstrated strong legislative momentum in school digital governance. The Cybersecurity Act 366/2024, mobile phone restrictions effective from January 2025, dedicated cyberbullying guidance (Guidance 1/2025), and a national AI-in-education plan for 2025 to 2027 reflect a comprehensive and structured approach. The school principal holds direct legal accountability for cybersecurity under Slovak law. The DigiEDU/DigiNET infrastructure programme provides secure, centralised internet connectivity to all Slovak schools.

Area	What It Means for Schools
NIS2 Transposition Act 366/2024 Act 69/2018	• Act 366/2024 directly links cybersecurity obligations to the school principal's statutory responsibility under Act 596/2003 on Schools. The principal is personally and legally accountable for protecting school information systems and personal data. • Schools must implement basic security measures: strong passwords, antivirus software, regular updates, data backups, and access controls. • Schools must be able to respond to phishing attacks, ransomware, data leaks, and system compromises. • Mandatory reporting procedures must be followed for serious cybersecurity incidents. • Act 69/2018 provides the foundational framework for protection of information systems and networks, ensuring the security of student data and safe use of digital technologies in schools.

Area	What It Means for Schools
Data Protection Act 18/2018	• A DPO is mandatory for public schools but does not need to be one per school: a shared DPO across multiple schools is permitted. • Schools must apply data minimisation: only collect and use personal data of students that is strictly necessary for education and administration. • Access to data must be limited to authorised persons (teachers, management, administration) as needed. • Electronic systems, emails, paper documents, and storage devices must be protected from loss or unauthorised access. • Photos, student lists, results, or sensitive information must not be published without a legal basis or explicit consent. • Any data protection breach must be reported to the relevant authority within 72 hours if it poses a risk to individuals.
Age of Digital Consent	• 16 years. • Parental or guardian consent is required before enrolling students under 16 on digital platforms.
Cyberbullying Guidance 1/2025	• Guidance 1/2025 provides specific rules on cyberbullying prevention and resolution in schools and educational facilities. • Defines the basic signs, forms, and manifestations of cyberbullying. • Sets out prevention procedures and methods for dealing with incidents. • Includes procedures for supporting victims. • Schools must implement the procedures set out in this guidance.
Mobile Phones Act 245/2008 (amended from January 2025)	• Students in grades 1 to 3 are not permitted to use mobile phones or similar devices at all during school. • Students in grades 4 to 9 may use them only for educational purposes when the teacher specifically permits it. • An exception applies to students with disabilities who use the device in connection with their health condition. • In the event of a violation, the school may temporarily confiscate the device. • Detailed conditions are governed by the school's internal regulations.
AI in Education AI Plan 2025-2027	• The Ministry of Education's Plan for the Responsible Use of AI in Education 2025-2027 provides practical national guidance for schools. • Schools should use this plan alongside the EU AI Act to assess and govern any AI tools they introduce. • Emphasis is placed on safety, ethical use, and transparency.
Digital Infrastructure	• DigiEDU/DigiNET: secure, centrally managed internet connectivity programme for all Slovak schools.

Area	What It Means for Schools
	• Cybersecurity is overseen by the National Security Office (NBU), which operates SK-CERT for incident response. • NBU provides guidance and support for public institutions including schools.
Key Contacts	• Cybersecurity: NBU/SK-CERT (nbu.gov.sk) • Data Protection: UOOU (dataprotection.gov.sk)

International Standards and Schools

The practical recommendations in Part 3 of this policy are grounded in a set of internationally recognised management standards. This short section explains what those standards are and why they matter for schools. You do not need to be familiar with the standards themselves to follow the guidance in Part 3. What the standards provide is a tested and widely accepted foundation that gives this policy its structure and credibility.

Five standards are relevant here. They each address a different dimension of how schools can protect their students, their data, and their systems.

ISO/IEC 27001 is the international standard for information security management. It provides a framework for identifying what information a school holds, understanding the risks to that information, and putting the right measures in place to protect it. In a school context, this means student records, staff data, digital platforms, and all the systems that support teaching and administration. ISO 27001 does not prescribe specific technical solutions. Instead, it sets out a way of thinking about security systematically, making sure nothing important is overlooked. The practical actions in Sections 3.1 through 3.7 are all rooted in this framework.

ISO/IEC 27002 sits alongside ISO 27001 and provides the detailed controls that put information security into practice. Where ISO 27001 describes the management framework, ISO 27002 describes the specific measures: how to control access to systems, how to manage passwords, how to handle incidents, how to configure devices securely. Sections 3.2 and 3.3 draw most directly on this standard.

ISO/IEC 27701 extends the information security framework to cover the protection of personal data specifically. It connects directly to the GDPR and helps schools demonstrate that they are managing student and staff data responsibly. Section 3.1 is built on this standard.

ISO 22301 is the standard for business continuity management. For schools, this means being prepared for disruptions: a cyberattack, a system failure, a ransomware incident that locks access to student records. ISO 22301 encourages organisations to plan in advance for these situations, to have backups and recovery procedures in place, and to test them regularly so that they work when needed. A school that follows this approach can recover quickly from an incident rather than facing weeks of disruption. Section 3.2 and the incident response procedure in Appendix IV reflect this standard.

ISO 31000 is the standard for risk management. It provides a way of thinking about risk that applies across all areas of school life, not just cybersecurity. Before adopting a new digital platform, before introducing an AI tool, before changing how student data is handled, a school should ask: what could go wrong, how likely is it, and what would the consequences be? This is the thinking that underlies the DPIA process in Appendix V, the platform assessment approach in Section 3.3, and the broader risk-aware approach throughout Part 3.

Together, these five standards provide the backbone of Part 3. They are the reason the recommendations in this policy are not arbitrary. They represent decades of accumulated knowledge about how organisations can protect their information, manage their risks, and keep operating when things go wrong. The guidance that follows translates that knowledge into practical steps that any school can take.

Part 3: What Your School Should Do

This part is organised into seven areas. Each area starts with a short explanation of why it matters, followed by a table showing what your school needs to do, why each action is important, and how to carry it out.

The recommendations in this section are most effective when they involve the whole school community. School leaders, teachers, administrative staff, students, parents, and external support organisations all have a role to play in creating a safe digital environment. Regular communication, practical education, and trusted reporting channels help schools build a culture of cyber resilience rather than simply responding to incidents.

3.1 Protecting Personal Data

Schools hold a large amount of personal information about students, parents, and staff. This includes names, ID numbers, attendance records, grades, health information, and family contact details. Protecting this data is a legal obligation. It is also a matter of trust. Families share sensitive information with schools because they have to. Schools have a responsibility to handle it carefully.

When data protection goes wrong, the consequences can be serious. Student information may be exposed to people who should not have it. The school may face a formal investigation. And the trust of students and families can be difficult to rebuild. Getting the basics right from the start is far easier than dealing with the aftermath of a breach.

What	Why It Matters	How to Do It
Appoint a Data Protection Officer (DPO)	The DPO is the person responsible for making sure your school complies with data protection law. Without one, there is no clear accountability when something goes wrong. The DPO is also the main contact for students, parents,	Check Part 2 to find out whether your school needs its own DPO or whether the role is covered at cluster or authority level. The DPO must be accessible to staff, students, and parents. They are responsible for monitoring compliance, advising on data protection questions, training staff, and liaising with the supervisory authority.

What	Why It Matters	How to Do It
	and the national supervisory authority.	
Keep a record of all data processing activities	This record is required by law under GDPR Article 30. It shows what personal data your school holds, why it holds it, who can access it, and how long it is kept. If the supervisory authority asks for it, you need to be able to produce it.	The register must cover every category of personal data your school processes: student records, parent contacts, staff data, health information, and so on. For each category, record the purpose, the legal basis, who has access, how long it is kept, and what happens when it is no longer needed. The DPO is responsible for keeping it up to date.
Only collect the data you actually need	Every piece of data you collect is a risk. If there is a breach, only data you actually hold can be exposed. Collecting more than you need also means more work to manage and more potential for non-compliance.	Go through all your data collection forms, enrolment processes, and platform settings. Remove any fields that ask for information the school does not genuinely need. If a platform asks for more data than necessary, push back on the supplier or choose a different platform. Make it the rule that optional data collection is turned off by default.
Sign agreements with every supplier that processes student data	When a company processes student or staff data on your behalf, for example a cloud platform, a grading tool, or a communication app, your school remains legally responsible for how that data is handled. Without a written agreement, you cannot demonstrate you have met your obligations.	Before any supplier goes live with a service that involves personal data, they must sign a Data Processing Agreement. This must specify what data is processed, for what purpose, what security measures are in place, and what happens to the data when the contract ends. Keep copies of all agreements on file.
Limit who can access personal data	The more people who have access to data, the greater the risk of it being misused, accidentally disclosed, or stolen. Every unnecessary access point is a vulnerability.	Set up role-based access so that each member of staff can only see the data they need for their specific job. A teacher should see their own students' records, not those of the whole school. Administrative staff should access administrative data, not health or psychological files. Review who has access at least once a year, and remove access immediately when someone changes role or leaves.
Tell students and parents how their data is used	Students and parents have a legal right to know what data is held about them and how it is used. Providing this	Write a privacy notice in plain language that any parent or older student can understand. It must explain what data is collected, why, who can access it, and how long it is kept. Provide it

What	Why It Matters	How to Do It
	information is not optional. Schools that are transparent about data use also tend to have fewer disputes and complaints.	when students enrol and whenever something significant changes. Make it permanently available, for example on the school website. A template letter is in Appendix II.
Get parental consent for students below the age of digital consent	For students below the national age of digital consent, you cannot enrol them on a digital platform without written consent from a parent or guardian. This is a legal requirement. The age varies between 13 and 16 across the five countries, which means the same platform may require consent in one country but not in another.	Set up a clear process for collecting, recording, and renewing parental consent. Consent must be specific to each platform, freely given, and easy to withdraw. Do not assume that signing a general enrolment form covers all digital platforms. Check the age of digital consent for your country in Part 2.
Report data breaches within 72 hours	The 72-hour deadline is a hard legal requirement. If your school discovers a breach and does not report it on time, or tries to handle it quietly without telling the supervisory authority, the consequences can be significantly worse than if the breach had been reported promptly.	Put a written breach response procedure in place before anything happens. When a breach occurs, the DPO must immediately assess whether it creates a risk to individuals. If it does, the national supervisory authority must be notified within 72 hours. If the risk is high, the affected individuals must also be notified directly. Use the incident log in Appendix IV to record every step.

What is a data breach?

A data breach is any incident that results in personal data being accidentally or unlawfully lost, destroyed, changed, disclosed, or accessed by someone who should not have it. This includes a USB drive containing student records that goes missing, an email sent to the wrong person, a ransomware attack that locks school data, or a platform setting that accidentally makes student records publicly visible. Many of the most common breaches in schools are caused by human error, not external attacks.

3.2 Keeping School Systems Secure

Cybersecurity means protecting your school's computers, networks, and data from attacks and unauthorised access. Schools are an attractive target for cybercriminals because they hold sensitive data about children and often have limited security resources. A successful attack can shut down school systems, expose student records, disrupt learning for weeks, and cause lasting damage to the school's reputation.

The good news is that most successful cyberattacks exploit simple weaknesses that can be fixed without specialist expertise or large budgets. Weak passwords, software that has not been updated, staff who do not recognise phishing emails, and missing backups are behind the majority of incidents. Fixing these basics makes an enormous difference.

Equally important is being prepared for the moment when something does go wrong. Having a tested backup and a clear recovery procedure means the difference between a disruption that lasts a few hours and one that lasts weeks. This is the thinking behind business continuity planning: not just preventing incidents, but making sure the school can keep functioning and recover quickly when they occur.

What	Why It Matters	How to Do It
Use strong passwords and multi-factor authentication	Weak passwords are the most common way attackers get into school systems. A password that is easy to guess, or one that is used on multiple accounts, means that one stolen password can give an attacker access to everything. Multi-factor authentication adds a second check that protects accounts even when a password is stolen.	All staff accounts must use strong passwords of at least 12 characters, combining letters, numbers, and symbols. Passwords must be changed if there is any reason to think they have been compromised. Multi-factor authentication must be turned on for all systems that hold student data. After entering their password, the staff member must confirm their identity through a second method, such as a code sent to their phone.
Keep all software and devices up to date	Software updates often include fixes for security weaknesses that attackers are actively exploiting. Many of the worst ransomware attacks on schools have targeted systems running old software that had not been updated. This is one of the most preventable vulnerabilities there is.	Set up a regular schedule for applying updates to all school devices, operating systems, applications, and security software. Apply critical security patches as soon as they are available. If a device can no longer receive updates, remove it from the network or replace it. Assign a specific member of staff responsibility for making sure updates happen.
Back up all important data regularly	Ransomware attacks work by encrypting your data and demanding payment to restore access. The only reliable way to recover without paying is to have a backup that was made before the attack. Without a tested backup, a school can lose weeks of work and permanent records.	Set up automated daily backups for all critical school data. Keep at least one copy of each backup in a location that is not connected to the school's main network, so it cannot be encrypted in the same attack. Test the recovery process at least once a year to confirm that the backups actually work and that data can be restored in a reasonable time.

What	Why It Matters	How to Do It
Use separate networks for administration and students	If the network used by administrative staff, where student records and grades are managed, is the same as the one used by students and visitors, then a compromised student device or an infected visitor laptop could potentially reach school administrative systems. This is a basic risk that network separation removes.	Set up separate Wi-Fi networks: one for administrative use and one for students and visitors. Make sure the administrative network is not visible or reachable from the student network. Set up access controls so that only authorised school devices can connect to the administrative network.
Protect all school devices	Devices that have default factory passwords, have never been updated, or have no antivirus protection installed are easy targets. Many schools have devices in classrooms or offices that were set up years ago and have not been reviewed since.	Install antivirus and antimalware software on all school devices and keep it updated. Change all default passwords on routers, cameras, printers, and any other connected equipment as soon as it is installed. Carry out a regular audit of all connected devices. Before disposing of old devices, make sure all data has been permanently and securely deleted.
Have a written plan for dealing with incidents	Without a written plan, staff who find themselves dealing with a cyberattack will not know what to do. Panicked or well-meaning but wrong decisions, such as turning off a device immediately or trying to pay a ransom, can make a bad situation much worse.	Write a cyber incident response procedure that sets out who coordinates the response, what steps to take and in what order, which national authorities to contact and within what timeframe, and how to communicate with students, parents, and staff during and after an incident. Make sure all relevant staff know the procedure before an incident happens. A template is provided in Appendix IV.
Train all staff at least once a year	Phishing emails are behind the majority of successful cyberattacks on schools. A staff member who cannot recognise a phishing email is a vulnerability that no technical system can fully protect against. One click on a malicious link can give an attacker full access to school systems.	Provide mandatory annual cybersecurity awareness training for all staff. Training must cover how to spot a phishing email, how to create and manage strong passwords, what to do if a device is lost or stolen, and who to contact if something looks wrong. Add periodic reminders throughout the year. Where possible, run simulated phishing exercises: these are one of the most effective ways to change staff behaviour.

What is a phishing attack?

Phishing is when an attacker sends an email, message, or notification that looks like it comes from someone trusted, such as the Ministry of Education, a software provider, or a colleague. The goal is to get the recipient to click on a malicious link, enter their login details on a fake website, or open an infected file. Phishing is the most common form of cyberattack against schools. Any unexpected message asking for a password, asking someone to click a link urgently, or asking them to take an unusual action should be treated with suspicion and verified through a separate channel before anyone responds.

3.3 Choosing and Using Digital Platforms Safely

Schools use a growing number of digital platforms for teaching, communication, and administration. Each platform that processes student data is a potential source of risk. A platform that has weak security, shares data with advertisers, or stores student information outside the EU without proper safeguards can cause real harm. Schools have a legal duty to check platforms before adopting them and to manage them carefully once they are in use.

The same applies to artificial intelligence tools. AI is increasingly present in education, but not all tools are safe to use with students. The EU AI Act draws clear lines, and schools need to know where those lines are before introducing any AI tool in the classroom or in processes that affect students.

What	Why It Matters	How to Do It
Check every platform before using it	A platform that is adopted without proper checks may process student data in ways the school has not agreed to, store data outside the EU, or have security weaknesses. Once data has been shared with the wrong provider, it is very hard to undo.	Before adopting any new platform, verify that it complies with the GDPR, that it does not use student data for advertising or share it with third parties without consent, and that it stores data within the EU. If the platform involves large-scale processing of student data, complete a DPIA before going live (see Appendix V). Sign a data processing agreement with the provider before any data is shared.
Keep a list of approved platforms	Without a central record, schools lose track of what platforms are in use, when they were last checked, or who approved them. Staff may start using platforms informally without any assessment. Students may use personal accounts on unapproved tools for school work, taking data outside the school's control.	Keep a written register of all digital platforms and tools approved for use in your school. Record the name of the platform, what it is used for, when it was assessed, and when the next review is due. Review the register at least once a year. Staff must not introduce new platforms for school use without going through the approval process first.

What	Why It Matters	How to Do It
Set platforms up securely	Default settings on platforms are usually designed for ease of use, not for security. A virtual classroom that anyone can join without logging in, a recording function that is on by default, or student accounts with excessive permissions all create risks that are easy to avoid.	Every platform must be configured securely before students or staff start using it. Video conferencing tools must require a login before anyone can join a virtual classroom. Recording must be off by default and only turned on with the explicit consent of everyone present. Student accounts should have only the permissions they need for their educational activities. Check the settings at least once a year.
Know which AI uses are prohibited	Some AI practices in educational settings are banned by EU law. This applies regardless of how the tool was marketed or what the vendor claims. The prohibition is absolute and applies to all schools in all five countries.	Do not use any AI tool that involves recognising students' emotions, categorising them biometrically, or identifying them in real time through facial recognition. These uses are prohibited under Article 5 of the EU AI Act. If a vendor offers these features, the school must not use them. If the school is already using such a tool, it must stop.
Keep humans in charge of decisions about students	AI tools can produce recommendations that are wrong, biased, or unfair. When these recommendations influence what happens to a student, such as a grade, a referral, or an assessment of learning needs, the consequences can be serious. The law requires a human to be in charge for precisely this reason.	A teacher or responsible adult must always review and take responsibility for any output from an AI tool that affects a student. AI tools can assist, but they cannot make final decisions. Document how human oversight is applied for each AI tool that is used in educational decision-making.
Tell students and parents when AI is being used	Students and parents have a right to know when AI tools are used in ways that affect a student's education. Using AI tools without informing them is likely to be a breach of both the AI Act and the GDPR.	When an AI tool is used in a way that affects a student's learning or assessment, inform students and parents clearly and in plain language: what the tool does, what data it uses, how its outputs are used, and how human oversight works. Provide this information before the tool is used and keep it permanently accessible.
Keep a record of all AI tools in use	Schools that do not know what AI tools they are	Maintain an AI tools register as part of your approved platforms list. For each AI tool,

What	Why It Matters	How to Do It
	using, what data those tools process, or what assessment was done before adoption cannot meet their legal obligations under the AI Act or the GDPR.	record what it does, what risk category it falls into under the AI Act, what data it processes, what assessment was carried out before adoption, and who is responsible for oversight. Review this record at least once a year.

3.4 Managing Mobile Phones and Personal Devices

All five partner countries have introduced legal restrictions on mobile phone use in schools. The specific rules differ by country (see Part 2), but the reasons are the same everywhere: phones in classrooms distract students from learning, create risks for privacy and data protection, make cyberbullying easier, and add to the digital pressures that affect student mental health.

A mobile phone policy is more than a disciplinary rule. It is a data protection measure, a wellbeing measure, and a statement of what the school values. A policy that is clearly written, genuinely understood by students, parents, and staff, and applied consistently is far more effective than one that exists only on paper.

What	Why It Matters	How to Do It
Have a clear, written mobile phone policy	Without a written policy, rules are applied differently by different teachers. Students and parents cannot be held to rules they were not clearly told about. Inconsistent enforcement creates conflict and undermines trust in the school's rules.	Write a mobile phone policy that covers when phones may and may not be used, where they must be stored during restricted times, what exceptions exist for medical needs or specific educational activities, and what happens if the rules are broken. Share the policy with students and parents at the start of each school year through the Acceptable Use Policy (Appendix III). Include it in the school's internal regulations.
Restrict phone use during lessons	Unrestricted phone use during lessons disrupts learning, creates opportunities for cyberbullying and unauthorised recording, and adds to the digital pressures that affect student wellbeing. Research consistently shows that students in schools with clear phone restrictions do better	Students must not use personal mobile phones during lessons unless a teacher has specifically authorised it for a particular educational activity. In countries where there is a legal prohibition, it must be enforced. Be clear about where phones must be stored during restricted times. Exceptions for medical needs must be documented.

What	Why It Matters	How to Do It
	academically and report higher wellbeing.	
Prohibit unauthorised recording	Unauthorised recordings of students, teachers, or other staff are a serious breach of privacy and may be a criminal offence under national law. Recordings shared online can cause lasting damage to the individuals involved and to the school. The popularity of short video platforms makes this a growing risk.	Make it absolutely clear to students and staff that recording anyone in the school without their explicit consent is forbidden, whether during lessons, in corridors, on trips, or at events. State the consequences clearly. Treat any unauthorised recording involving students or staff as a serious disciplinary matter and, where necessary, refer it to the appropriate authorities.
Apply security standards to personal devices used for school work	When a teacher uses a personal device to access school systems, the school's data protection is only as strong as the weakest link. A personal device with a weak password, outdated software, or student data stored locally is a real vulnerability.	Staff who use personal devices for school work must protect them with a strong password or PIN, keep their software updated, use a secure connection when working remotely, and not store student data locally on personal devices. Provide clear guidance to staff on what is expected.

3.5 Preventing and Responding to Cyberbullying

Cyberbullying is bullying that happens through digital devices and platforms. It includes sending threatening or humiliating messages, sharing private images without consent, spreading false information online, and deliberately excluding someone from online groups. Cyberbullying can cause serious and long-lasting harm to students' mental health, academic performance, and social relationships.

Schools have both a legal obligation and a duty of care to prevent cyberbullying and to respond when it happens. Cyberbullying does not stop at the school gate. What happens online at home in the evening can affect a student's experience in school the next morning, and the other way around. Schools must treat cyberbullying as seriously as physical bullying, even when it happens outside school hours.

What	Why It Matters	How to Do It
Include cyberbullying explicitly in your anti-bullying policy	A general anti-bullying policy that does not mention cyberbullying leaves room for doubt	Update your anti-bullying policy to include a dedicated section on cyberbullying. It should define what cyberbullying is, make clear it is treated as seriously as physical bullying, and confirm that the

What	Why It Matters	How to Do It
	about whether online behaviour is covered. Students who are bullied online may not report it because they think the school will say it is not their problem.	policy applies to online behaviour outside school hours when it directly affects the school community. Review the policy at least once a year.
Teach students about cyberbullying	Students who understand what cyberbullying is, why it causes harm, and what to do when they see it happening are more likely to report it and more likely to support a peer who is being targeted. Teaching students to be active, supportive bystanders is one of the most effective approaches there is.	Deliver age-appropriate cyberbullying education as a regular part of the curriculum, not as a one-off event. Cover what cyberbullying looks like on different platforms, the harm it causes, how to support someone who is being targeted, and how to report it. Involve students in shaping the content: they engage more with messages they have helped create.
Give students a clear and safe way to report	Many students who are being cyberbullied do not report it. They worry they will not be believed, that reporting will make things worse, or that they will lose access to their phone. Without a trusted and accessible reporting route, incidents stay hidden and get worse.	Offer more than one way to report cyberbullying: a trusted adult, an anonymous form or box, and where available, the national reporting platform (see Part 2). Actively promote these options throughout the school year, not just in September. When a student reports, respond quickly and make it clear you take it seriously.
Train all staff to recognise and respond to cyberbullying	Many teachers are unsure how to respond to cyberbullying, especially when it involves platforms they are not familiar with. Uncertainty leads to inconsistent responses, which undermine both the victim and the school's ability to manage incidents effectively.	Give all staff training that covers how to spot signs that a student may be experiencing cyberbullying, what the school's procedure is and what their role is in it, how to preserve evidence including screenshots, when to involve the school counsellor, parents, or external authorities, and how to support a student without inadvertently making things worse.
Respond quickly and document everything	A slow or inconsistent response sends a message that the school does not	When a cyberbullying incident is reported, the first priority is the safety and wellbeing of the student who was targeted. Write down the details

What	Why It Matters	How to Do It
	take cyberbullying seriously. It also allows incidents to escalate and evidence to be lost. Schools that do not keep proper records find it hard to spot patterns or to show that they acted appropriately if a formal complaint is made.	immediately: the date and time, what happened, which platforms were involved, who was involved, any evidence collected, and every action taken. Apply the disciplinary procedure consistently. Check in with the targeted student in the days and weeks after the incident.
Involve parents as partners	Parents who understand cyberbullying, know how to talk to their children about it, and feel connected to the school's approach are far more effective at both preventing incidents and supporting their children when incidents occur.	Tell parents at the start of the year about the school's approach to cyberbullying, what to do if their child is affected, and how the school will communicate with them. Use the template in Appendix II. When incidents occur, involve the parents of all students affected, following the school's procedures.

Schools do not have to address these challenges alone. Safer Internet Day (February) and European Cybersecurity Month (October) provide schools with ready-made awareness materials validated at EU level. The EU's Better Internet for Kids (BIK+) programme and the Insafe network of Safer Internet Centres operate helplines, reporting tools, and educational resources in all five partner countries that schools can draw on directly.

3.6 Supporting Students' Digital Wellbeing

Students face risks online that go beyond cyberbullying and data breaches. Many experience anxiety, low self-esteem, and social pressure connected to their digital lives. Fear of missing out, pressure to present an idealised version of themselves online, constant comparison with others, excessive screen time, and the design of social media platforms that prioritise engagement over wellbeing all contribute to mental health challenges that affect a significant number of young people.

Restricting access alone does not solve these problems. Students who are simply told to use technology less, without being helped to understand why or given tools to manage their own behaviour, tend to revert as soon as restrictions are lifted. Schools that see lasting positive change are those that combine clear boundaries with honest, evidence-based education and a culture where students feel safe to talk about what they experience online.

What	Why It Matters	How to Do It
Make digital wellbeing part of pastoral care	Students who are struggling with their online lives are struggling with their overall mental health and social experience. If digital wellbeing is treated as a separate IT topic, students who need support may fall through the gaps between services.	Digital wellbeing should be a named part of the school's wider wellbeing and pastoral care programme. The staff who support students through other challenges should also be ready to support them with digital ones. Referral routes should be clear: any teacher who identifies a student who is struggling should know exactly who to involve and what happens next.
Teach students healthy digital habits	Students who understand how social media platforms are designed to keep them scrolling, who can tell the difference between a curated online image and reality, and who have developed their own strategies for managing their digital habits are better placed to navigate the online world safely.	Include digital wellbeing education as a regular part of the curriculum. Teach students how recommendation algorithms work and why they often show content that triggers strong emotions. Discuss the effects of scrolling social media passively on mood and self-esteem. Help students develop practical strategies for setting boundaries around their own technology use.
Make sure students know where to get help	Many students who are struggling with something online do not ask for help because they do not know help is available, because they are embarrassed, or because they fear their phone will be taken away. If support is not actively promoted, it is invisible to the students who most need it.	Regularly remind students who they can talk to if something online is bothering them. Mention it in assemblies, in lessons, and in everyday interactions, not just in a handbook. The person a student approaches does not need to be a technology expert. They just need to be someone the student trusts, who will listen without judgement and connect them to the right help.
Do not add to digital pressure through school practices	Schools can inadvertently create the same digital pressures they are trying to reduce. Mandatory school group chats, expectations that students respond to messages outside school hours, and public comparisons between students online can all send unhelpful messages.	Review how the school communicates digitally and whether any of its own practices contribute to digital pressure. Avoid mandatory group chats that blur the line between school and personal time. Do not expect students or parents to respond to messages outside normal hours. Avoid publishing rankings or comparisons online.

What	Why It Matters	How to Do It
Recognise when a student is struggling	Students who are having difficulties with their digital lives may not say so directly. The signs are often behavioural and easy to miss unless staff know what to look for.	Give staff guidance on the signs that a student may be struggling with their digital life: unusual anxiety about not being able to check their phone, mood swings following online interactions, withdrawal from social activity after something that happened online, distress connected to their appearance or how others see them online, reluctance to come to school after an online incident, or any sign they are being pressured or targeted online. When these signs appear, staff should follow the school's pastoral referral procedure.

3.7 Diversity, Inclusion, and Digital Equity

Not all students face the same digital risks or have the same access to support. Gender, sexual orientation, disability, family income, and concerns about body image all shape a student's experience online and their ability to get help when something goes wrong. A policy that works well for most students but overlooks the experience of others is not complete.

Building an inclusive approach to digital safety means thinking actively about which students are most at risk and making sure the school's policies, education, and support systems reach them.

What	Why It Matters	How to Do It
Address gender-based and identity-based online harm explicitly	Girls face disproportionately high rates of online sexual harassment, image-based abuse, and cyberbullying linked to appearance. LGBTQ+ students are significantly more likely to experience online harassment and to suffer mental health difficulties as a result. Research finds that reported prevalence of cyberbullying among LGBTQ+ students varies widely: from roughly 10% to over 70% depending on context, and that LGB students report being cyberbullied at approximately double the rate of their heterosexual peers. Research shows that cyberbullying statistically mediates much of the elevated anxiety, depression, and loneliness reported by sexual-minority students, meaning that inclusive prevention is a central	Update the school's anti-cyberbullying policy to explicitly cover gender-based online harassment, sexual harassment, sharing of intimate images without consent, and harassment based on sexual orientation or gender identity. Make sure staff training covers these specific forms of harm and how to respond to them. Create a school environment where every student feels equally safe to report what is happening to them.

What	Why It Matters	How to Do It
	mechanism for protecting this group's mental health. A policy that does not name these specific forms of harm leaves the most vulnerable students without adequate protection.	
Make digital safety education accessible to students with disabilities	Students with disabilities, including learning differences, may be more vulnerable to online manipulation and exploitation. They may also find it harder to access digital safety education that is not designed with their needs in mind. If reporting mechanisms are not accessible to them, they effectively do not exist.	Make sure all digital safety education is delivered in ways that work for students with different learning needs. Check that digital platforms used in school meet accessibility standards. Make sure reporting mechanisms are accessible to students who communicate differently. Work with special educational needs staff to identify students who may need additional support in understanding and managing online risks.
Recognise and address the digital divide	Students from lower-income families may have limited or unreliable internet access at home, older or shared devices, and less adult support in navigating the online world. Students using shared devices face greater privacy risks. These students may also be less likely to recognise or report problems.	Do not design digital activities or communication practices that assume a level of home connectivity that not all students have. Be aware that students using shared devices face particular privacy risks and provide specific guidance. Make sure digital safety education reaches all students. Identify students who lack adequate home connectivity and address this through available national programmes.
Help students develop critical awareness of body image online	Social media constantly exposes students to edited, filtered images that set standards of appearance that are not realistic. This is associated with lower self-esteem and anxiety, particularly in adolescent girls, and in some cases with disordered eating.	Include education about body image and online appearance as part of the digital wellbeing curriculum. Teach students how images are edited and filtered before being posted, and help them understand that what they see online is a performance rather than reality. Discuss how platform algorithms amplify appearance-based content. Approach this topic sensitively. Some students may already be struggling. Make sure referral routes to specialist support are in place.
Apply an inclusive lens to all of this policy	A policy designed without considering the experiences of different groups of students will reflect the majority experience and leave others less protected. The	Go through every section of this policy and ask: does this reach the students who are most at risk? Are our reporting routes accessible to everyone? Does our staff training cover the specific vulnerabilities

What	Why It Matters	How to Do It
	students who face the greatest online risks are often those whose experiences have been least considered.	of different groups? Involve students, including those from underrepresented groups, in reviewing and improving the school's approach to digital safety.

Part 4: What the Evidence Shows

This part summarises what the research tells us about what actually works when schools address cybersecurity, cyberbullying, and digital wellbeing. Use this section to make informed choices about the programmes, approaches, and interventions your school adopts.

4.1 Cybersecurity Awareness and Training

Research on cybersecurity in schools consistently identifies human behaviour as the most important risk factor. Most successful attacks begin with a phishing email or a weak password. Technical defences help, but they cannot prevent an attack when staff are not trained to recognise the threat. This means that investing in staff training is at least as important as investing in technical tools.

Studies on staff cybersecurity training show that regular, practical training works significantly better than a single awareness session. Staff who receive annual training and occasional reminders are measurably less likely to click on phishing links or to use unsafe practices with school systems. The way training is delivered also matters: interactive sessions with real-world examples work better than passively reading information or watching a video.

Simulated phishing exercises, where staff receive a carefully designed fake phishing email to test how they respond, are among the most effective training methods available. Schools and organisations that run these exercises regularly see clear improvements in how staff behave over time. The exercise is most effective when it is followed immediately by feedback explaining what the signs were and what the right response would have been.

For students, the evidence shows that cybersecurity education works best when it is woven into the curriculum rather than delivered as a standalone event. Students who learn about online safety through real examples, interactive activities, and discussion with their peers absorb the lessons better and apply them more consistently in their own lives than students who receive the same information in a lecture.

4.2 Cyberbullying Prevention

The research on cyberbullying prevention consistently shows that whole-school approaches work best. This means programmes that bring together students, teachers, parents, and school leadership around a shared goal of creating a safer environment. Schools that treat cyberbullying purely as a disciplinary matter, to be dealt with after incidents occur, consistently get worse outcomes than schools that take a whole-community prevention approach.

Programmes that focus only on the behaviour of those who bully are less effective than those that also build empathy and bystander skills. Students who understand the harm cyberbullying causes and who

have been taught how to support a peer who is being targeted are more likely to report incidents and more likely to step in to help. Whether bystanders intervene or stay silent is one of the strongest predictors of whether bullying escalates or stops.

Anonymous reporting systems consistently lead to more incidents being reported. Students who experience cyberbullying often do not tell anyone because they are afraid they will not be believed, that things will get worse, or that there will be social consequences among their peers. Schools that offer a genuinely confidential and trusted reporting route see higher rates of disclosure and earlier intervention.

Teacher training is essential and often underestimated. Research shows that many teachers feel uncertain about how to respond to cyberbullying, particularly when it involves apps or features they are not familiar with. Schools that invest in practical, structured teacher training on recognising and responding to cyberbullying consistently see better outcomes for students.

Parental involvement also makes a consistent difference. Parents who understand cyberbullying, who know how the platforms their children use work, and who feel connected to the school's approach are better at both supporting their children and reinforcing the school's messages at home.

Research provides clear evidence of the scale of the problem. According to the WHO Health Behaviour in School-aged Children study (2024), around one in six adolescents in Europe, approximately 15%, reports experiencing cyberbullying, with rates broadly similar between boys and girls and an upward trend compared with 2018. OECD data found variation between countries ranging from around 7.5% to 27.1%. Helpline data from the EU's Insafe network consistently ranks cyberbullying among the most common reasons children and teenagers contact support services, and in Q4 2025 it was again the single most frequent issue raised.

When consulted by the European Commission in 2025, over 6,000 children and teenagers aged 12 to 17 across the EU expressed clear expectations of schools: a majority wanted explicit rules and consequences for cyberbullying, direct teaching on the topic, and psychological support for those affected. Girls were consistently more likely than boys to request these measures.

A meta-analysis by Polanin et al. (2021), covering more than 45,000 students, found that dedicated cyberbullying-prevention programmes produced a statistically significant reduction in both perpetration and victimisation, and that programmes designed specifically for cyberbullying outperformed general anti-bullying approaches.

4.3 Digital Wellbeing

The research on technology use and student mental health does not support simple conclusions. Not all technology use is harmful. Using technology actively for creative work, communication, or learning can have positive effects. The consistent problem is passive use: scrolling through social media without purpose or meaningful interaction. This type of use is most strongly associated with anxiety, loneliness, and lower self-esteem, with the effects being particularly marked in adolescent girls.

The evidence strongly supports education over restriction. Schools that focus exclusively on limiting access to technology, without helping students understand why certain patterns of use are harmful or giving them tools to manage their own behaviour, see less lasting change. Students who understand the problem and have developed their own strategies show more sustained improvements in wellbeing.

Programmes that teach students to think critically about their digital habits, to understand how social media platforms are designed to maximise engagement, and to recognise the gap between curated online images and reality have shown positive results in reducing anxiety and improving self-esteem across multiple studies. These programmes work best when they are delivered over time as part of the curriculum, rather than as a single event.

Involving students in creating school digital rules consistently increases both how much they comply and how much they feel ownership of the rules. Students who feel that the rules are fair and that they had a voice in shaping them are more likely to follow them and more likely to encourage their peers to do the same.

A particularly important finding concerns Fear of Missing Out (FOMO). Research increasingly conceptualises FOMO not as a passing mood but as a relatively stable psychological characteristic, a persistent anxiety about missing rewarding experiences that others are having. Studies associate FOMO with depressive symptoms, sleep disturbance, and compulsive checking behaviour. A 2025 systematic review and meta-analysis confirmed a consistent statistical association between social media dependence and higher levels of anxiety, depression, loneliness, and lower self-esteem, with FOMO frequently identified as a mediating factor. Schools should address FOMO and compulsive use patterns explicitly in student-facing activities, not only through generic screen time messaging.

Research also notes that outcomes depend heavily not just on how much students use digital platforms but on how they use them. Social media can function as a source of support for some students, particularly those who are isolated or belong to minority groups. Prevention approaches should help students develop a more conscious and intentional relationship with technology.

Early identification and referral matter. Students who are connected to the right support before their difficulties become serious show significantly better outcomes than those who are only identified when the problems are already visible through falling grades or serious behavioural changes. Schools that have clear, well-known pathways for spotting and supporting students who are struggling are in a much better position to help them.

Appendix I: National Reference Table

Use this table to find the key national parameters for your country. Where this policy says to check national rules, this is where to look.

Parameter	Greece	Italy	Portugal	Romania	Slovakia
Age of digital consent	15 years	14 years	13 years	16 years	16 years
Data protection authority	HDPA dpa.gr	Garante garanteprivacy.it	CNPD cnpd.pt	ANSPDCP dataprotection.ro	UOOU dataprotection.gov.sk
Cybersecurity authority	EAKE cyber.gov.gr	ACN acn.gov.it	CNCS cncs.gov.pt	DNSC dnsc.ro	NBU nbu.gov.sk
Reporting cyber incidents	EAKE	ACN	CERT.PT (24h for NIS2)	DNSC/PNRISC (24h)	NBU/SK-CERT
Reporting data breaches	HDPA, 72 hours	Garante, 72 hours	CNPD, 72 hours	ANSPDCP, 72 hours	UOOU, 72 hours
Cyberbullying resource	stop-bullying.gov.gr	Report to school or police	seguranet.pt	School or ANSPDCP	Guidance 1/2025
Mobile phone law	Strict ban 2018/2024	All cycles 2024/25	Years 1-6 from Sept 2025	During class, Law 198/2023	All grades from Jan 2025
AI guidelines for schools	EU AI Act only	MD 166/2025	Not yet issued	Not yet issued	AI Plan 2025-2027

Appendix II: Template Letter to Parents

Schools can adapt this letter to inform parents about how the school handles student data and what it does to keep students safe online. Send it at enrolment and whenever significant changes are made to the school's digital systems or policies.

[School Name and Address]

[Date]

Dear Parent / Guardian,

How We Protect Your Child's Data and Support Their Digital Safety

We are writing to tell you how our school handles personal data about students and what we do to keep your child safe in their digital learning environment.

What data we collect and why. We collect personal information about your child that is necessary for education and administration. This includes their name, identification number, attendance records, and grades. In some cases we may also hold health-related information where it is relevant to their education. We only collect what we need and keep it for as long as the law requires.

Who can access it. Access to your child's personal data is limited to authorised staff members who need it to do their jobs. We do not share data with outside parties unless the law requires it or you have given your explicit consent.

Digital platforms. Our school uses digital platforms for teaching and administration. Before adopting any platform, we check that it complies with the GDPR. Your child will access these platforms through a school-issued account. A list of the platforms we currently use is available from the school office.

Your consent. For students below the age of [insert national age of digital consent], we need written parental consent before we can enrol your child on a digital platform. You will be asked to give this at enrolment and whenever a new platform is introduced.

Cyberbullying. Our school has clear procedures for preventing and responding to cyberbullying. If your child experiences or sees cyberbullying, please encourage them to speak to a trusted adult at school or contact us directly at [contact details].

Your rights. You have the right to see the data we hold about your child, to ask for corrections, and in some circumstances to ask for it to be deleted. To do this, please contact our Data Protection Officer at [DPO contact details].

Supporting digital wellbeing at home. We encourage you to talk regularly with your child about their online experiences, without judgement. If your child seems distressed or unusually anxious about their phone or online interactions, please contact [school counsellor / designated contact]. National helplines are also available for children and young people in your country.

If you have any questions, please do not hesitate to get in touch.

Yours sincerely,

[Principal's Name and School]

Appendix III: Acceptable Use Policy Template

Adapt this template to create your school's own Acceptable Use Policy. It should be signed by students, parents or guardians, and staff at the start of each school year. Adjust it to reflect your school's systems, national rules, and context.

Acceptable Use Policy

[School Name] | Academic Year [XXXX-XXXX]

1. Purpose

This policy sets out the rules for using digital devices, the internet, and digital platforms at our school. It applies to all students, staff, and visitors who use school systems. By signing this policy, you confirm that you have read and understood these rules and agree to follow them.

2. What you can use school digital resources for

- Completing schoolwork and educational activities
- Communicating with teachers and classmates for school purposes
- Using platforms that have been approved by the school
- Educational activities that a teacher has specifically authorised

3. What you must not do

- Access, create, or share content that is illegal, harmful, offensive, or discriminatory
- Bully, harass, threaten, or humiliate other students or staff through digital means
- Share personal information about other students or staff without their consent
- Record video or audio of students, teachers, or staff without their explicit consent
- Use another person's account or share your login details
- Install software or applications on school devices without authorisation
- Use personal accounts on unapproved platforms for school activities

4. Mobile phones

[Describe your school's mobile phone rules here, in line with the national law for your country as described in Part 2 of this policy. State where phones must be stored, what exceptions apply, and what happens if the rules are broken.]

5. Social media

Students must not post content about the school, other students, or staff that is harmful, misleading, or that could damage anyone's reputation. Online behaviour that amounts to cyberbullying, whether inside or outside school hours, is covered by this policy and by the school's anti-bullying procedures.

6. Reporting

If you come across content that makes you or another student feel unsafe, or if you see a violation of this policy, report it to a trusted adult at school or to [reporting contact].

7. Consequences

Breaking this policy may result in having access to school systems suspended, other disciplinary action under the school's disciplinary rules, and in serious cases, referral to law enforcement.

Student full name	
Student signature	
Parent or guardian name	
Parent or guardian signature	
Date	

Appendix IV: Cyber Incident Response Procedure

Follow these steps whenever a cyber incident occurs at your school. A cyber incident is any event that compromises the security, availability, or confidentiality of school data or systems. This includes a ransomware attack, unauthorised access to school systems, or a personal data breach.

Step 1: Identify and contain

As soon as someone discovers an incident, they must tell the school's IT coordinator or principal immediately. Do not try to fix the problem alone. Disconnect the affected device from the network by unplugging the cable or turning off Wi-Fi. Do not switch the device off unless you are specifically told to do so, as this can destroy evidence. Write down the time and a description of what you observed.

Step 2: Assess

The IT coordinator and DPO must assess the incident together. Work out which systems, accounts, or data have been affected. Determine whether personal data has been or may have been compromised. Check whether the incident is still ongoing or has been contained.

Step 3: Notify

If this has happened...	You should...
Personal data has been or may have been compromised	Notify the national data protection authority within 72 hours. See Part 2 for the authority in your country.
A significant cybersecurity incident has occurred	Notify the national cybersecurity authority. In Portugal, for entities covered by NIS2, this must be done within 24 hours. See Part 2 for your country's authority.
Criminal activity is involved	Contact the police.
Students or staff are at immediate risk or have been directly harmed	Provide support immediately and notify parents or guardians as appropriate.

Step 4: Recover

Restore systems from backups where available. Reset all affected passwords and access credentials straight away. Apply any relevant security updates before putting systems back into use. Check that restored systems are working correctly before making them available to students and staff again.

Step 4a: Support those affected

Provide immediate psychological and practical support to any student or staff member directly affected by the incident. This should happen in parallel with the technical response, not after it. Contact the school counsellor or pastoral care team without delay. Follow the school's wellbeing protocol.

Step 5: Review

Once the incident has been resolved, carry out a full review. Write down what happened, how it occurred, what was done, and what the outcome was. Identify what changes would reduce the risk of it happening

again. Brief the relevant staff on the findings, especially if the incident involved a phishing email or human error. Update the incident response procedure if needed.

Incident log

Date and time of incident	
How was it discovered and by whom?	
What happened?	
Which systems and data were affected?	
Immediate actions taken	
Was personal data compromised?	
Data protection authority notified? (Date)	
Cybersecurity authority notified? (Date)	
Police contacted? (Date)	
Recovery actions taken	
Date systems restored	
Review completed? (Date)	
Changes made as a result of the review	

Appendix V: Data Protection Impact Assessment (DPIA) Template

A DPIA is required before your school introduces a new digital system or platform that involves processing large amounts of student data, monitoring students systematically, automated decision-making that affects students, or sensitive categories of data. If you are unsure whether a DPIA is needed, ask your DPO.

Part A: What will be processed

Name of the system or platform	
Provider or vendor	
What personal data will be processed?	
Who are the data subjects? (students, staff, parents)	
What is the purpose of the processing?	
What is the legal basis for processing?	
Where will data be stored? (country, within EEA?)	
Who will have access?	
How long will data be kept?	
Will data be shared with third parties?	

Part B: Risk assessment

Risk	Level (Low / Medium / High) and how it will be addressed
Unauthorised access to student data	
Data lost or accidentally deleted	
Data used for purposes other than the original	
Students monitored or profiled without transparency	

Risk	Level (Low / Medium / High) and how it will be addressed
Data transferred outside the EEA without safeguards	
Data kept longer than necessary	

Part C: Decision

Overall risk level (Low / Medium / High)	
Can processing go ahead? (Yes / Yes with mitigations / No)	
What needs to be done before processing can start?	
DPO consulted? (Yes / No / Date)	
Assessment completed by	
Date of assessment	
Date of next review	

Appendix VI: School Risk Register

The School Risk Register helps your school identify, assess, and manage the key cybersecurity and data protection risks it faces. Completing this register is a practical step in implementing the risk management approach described in Part 3 of this policy.

The examples in the table below are indicative. They are provided to help your school get started and to illustrate the kind of risks that are most common in a school environment. Your school should add, remove, or adapt entries to reflect its own specific circumstances, systems, and context. The register should be reviewed at least once a year and updated whenever a significant change occurs, such as the introduction of a new digital platform or a cybersecurity incident.

How to score risks

For each risk, score Likelihood and Impact on a scale from 1 to 5 (1 = very low, 5 = very high). Multiply the two scores to get the Risk Score.

High risk (15-25): must be addressed immediately.

Medium-High risk (8-14): must be addressed, prioritise those with high impact.

Medium-Low risk (4-7): should be addressed where impact is significant.

Low risk (1-3): acceptable, monitor regularly.

An indicative Risk Register table is on the following page (landscape).

ID	Risk	What Could Happen	How We Reduce It	Likelihood (1-5)	Impact (1-5)	Risk Score	Responsible	If It Happens
1	Phishing email targeting staff	Staff click a malicious link, giving an attacker access to school systems and student data	Annual staff training, simulated phishing exercises, multi-factor authentication on all accounts	4	4	16	Principal / IT Coordinator	Isolate affected device, notify national cybersecurity authority, restore from backup
2	Ransomware attack	School systems are locked, student records and grades become inaccessible	Regular tested backups stored offline, up-to-date antivirus software, staff training	3	5	15	IT Coordinator	Restore from backup, report to national cybersecurity authority, notify data protection authority if student data is affected
3	Student data sent to the wrong person by mistake	Personal data about a student is accidentally shared with an unauthorised person	Staff training on data handling, use of official school communication channels only	4	3	12	DPO	Contact the recipient and request deletion, report to the national data protection authority within 72 hours if required, document the incident
4	Cyberbullying via school platform	A student uses a school communication tool	Acceptable Use Policy signed by all students and parents, cyberbullying	4	3	12	Principal / Form Teacher	Follow the school anti-bullying procedure, support the student affected, involve

ID	Risk	What Could Happen	How We Reduce It	Likelihood (1-5)	Impact (1-5)	Risk Score	Responsible	If It Happens
		to harass another student	education, clear reporting pathway					parents, document the incident

Appendix VII: Data Mapping Register

The Data Mapping Register helps your school record all the personal data it processes. Keeping this register is a legal requirement under GDPR Article 30. It must be available to the national data protection authority on request.

The examples below cover the most common categories of personal data processed by schools. They are indicative: your school should add any additional categories that apply to your own situation and remove any that do not. Review and update the register at least once a year and whenever a new system or platform is introduced.

What is a legal basis?

Every time your school processes personal data, it must have a lawful reason. The most common ones for schools are:

Legal obligation: processing required by national education law (e.g. keeping attendance records).

Public task: processing necessary for the school to carry out its public functions.

Consent: the person has agreed to the processing (required for photos, non-essential platforms).

An indicative Data Mapping Register table is on the following page (landscape).

Type of Data	Why We Process It	Legal Basis	Where It Is Stored	Who Has Access	How Long We Keep It	Backed Up?	Shared With
Student personal data (name, ID, address, date of birth)	Required for school administration and compliance with national education law	Legal obligation	National school information system (e.g. MySchool, SIIIR, Unica)	Principal, administrative staff only	As required by national law	Yes	Ministry of Education via national platform
Student academic records (grades, attendance, assessments)	Required to track student progress and report to parents	Legal obligation / Public task	School information system and teacher gradebook	Class teachers, principal, administrative staff	As required by national law	Yes	Parents (via secure channel), Ministry of Education
Student health information (allergies, disabilities, medical needs)	Necessary to protect student health and safety during the school day	Legal obligation / Vital interests	Secure paper file or encrypted digital record	Principal, school nurse, relevant teachers only	Duration of enrolment plus as required by law	Yes (encrypted)	Healthcare providers where necessary only
Student photos and images	School ID, publications, events documentation	Parental consent	School server or approved platform	Administrative staff, teachers with authorisation	Duration of enrolment; deleted on request	Yes	No third-party sharing without further consent

Appendix VIII: Registry of School Policies and Procedures

This registry helps your school keep track of the key security and data protection policies it has in place. Having documented policies in each of these areas is an important sign that the school is managing its cybersecurity and data protection responsibilities in a structured way.

The policies listed below are the ones most relevant to the recommendations in this Cyber Resilience Policy. The list is indicative: your school may have additional policies that should also be recorded here. For each policy, note who is responsible for it, when it was last updated, and when it is next due for review. Where a policy does not yet exist, record this as a priority action.

Templates available

Templates for several of the policies listed below are included in the appendices of this policy:

- Acceptable Use Policy: Appendix III.
- Incident Response Procedure: Appendix IV.
- Data Protection Impact Assessment (DPIA): Appendix V.
- Risk Register: Appendix VI.
- Data Mapping Register: Appendix VII.
- School Cyber Resilience Self-Assessment: Appendix IX

ID	Policy Name	Key Areas Covered	Policy Owner	Last Updated	Next Review
1	Acceptable Use Policy (AUP)	Use of school systems and devices. Mobile phone rules. Reporting.	Principal / IT Coordinator		
2	Access Control Policy	Who can access which systems and data. Password rules. Removal of access when a staff member leaves.	IT Coordinator / DPO		
3	Data Protection Policy	GDPR compliance. DPO responsibilities. Parental consent. Privacy notices. Data breach response.	DPO / Principal		

ID	Policy Name	Key Areas Covered	Policy Owner	Last Updated	Next Review
4	Backup Policy	What is backed up, how often, where it is stored, and how recovery is tested.	IT Coordinator		
5	Incident Response Policy	How the school responds to cybersecurity incidents and data breaches. Who is responsible. How to notify authorities.	Principal / DPO / IT Coordinator		
6	Anti-Bullying Policy (including Cyberbullying)	Definition of cyberbullying. Reporting pathway. How the school responds. Staff training. Parent involvement.	Principal		
7	Mobile Device Policy	Student mobile phone rules in line with national law. Prohibition on unauthorised recording.	Principal		

Appendix IX: School Cyber Resilience Self-Assessment

Schools can use this checklist to establish a baseline understanding of their current cyber resilience and identify priority gaps. Mark each item as Yes, Partially, or No. The purpose is not to pass or fail but to identify where to focus efforts.

Schools are encouraged to repeat this self-assessment at least once a year. Tracking scores over time helps monitor progress and supports a culture of continuous improvement.

The items listed are indicative. Adapt them to reflect your school's own context, national requirements, and specific circumstances.

Domain	What to check	Yes / Partially / No
Governance	The school has a designated cybersecurity or digital safety coordinator.	
Governance	The school has a written Acceptable Use Policy, reviewed within the last 2 years.	
Governance	The school has a documented incident response procedure known to staff.	
Awareness and Training	Staff receive at least annual training on cybersecurity and online safety.	
Awareness and Training	Students receive age-appropriate digital citizenship and online safety education.	
Awareness and Training	Parents and guardians receive information on digital risks at least once per school year.	
Wellbeing and Prevention	The school has a specific, named protocol for responding to cyberbullying.	
Wellbeing and Prevention	Students know how and to whom to report online incidents confidentially.	
Wellbeing and Prevention	Prevention activities explicitly address diverse and vulnerable groups.	
Data and Privacy	The school maintains a register of platforms and tools that process student data.	
Data and Privacy	Parental consent is obtained before enrolling students on digital platforms where legally required.	
Technical Measures	School devices and networks use up-to-date protective software and access controls.	
Technical Measures	Backups of critical school data are taken regularly and tested.	

How to interpret your score

Count Yes responses (1 point) and Partially responses (0.5 points). Divide by 13 and multiply by 100 for a percentage. Map to the maturity levels below.

Level	Score	Description
1 - Initial	0 to 20%	Little or no formal governance, training, or incident procedures in place.
2 - Developing	21 to 45%	Basic policies exist but are not consistently applied, reviewed, or communicated.
3 - Established	46 to 70%	Core governance, training, and incident response elements are in place and known to staff.
4 - Advanced	71 to 90%	Comprehensive, regularly reviewed policies and training reach staff, students, and parents.
5 - Resilient	91 to 100%	Cyber resilience is embedded in school culture with continuous training and inclusive prevention.

These levels are a self-assessment tool only and do not constitute formal certification or compliance assessment.

References

European Union Legislation

The following European Union legal instruments constitute the common legal framework underpinning this Policy. They establish the principal requirements for data protection, cybersecurity, artificial intelligence, digital services, electronic communications, and digital education across all EU Member States.

- European Union, Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- European Union, Directive (EU) 2022/2555 (NIS 2 Directive), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
- European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
- European Union, Regulation (EU) 2022/2065 (Digital Services Act), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
- European Union, Directive 2002/58/EC (ePrivacy Directive), Official Journal of the European Communities. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058
- European Union, Regulation (EU) 2019/881 (Cybersecurity Act), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

National Legislative Instruments

The following national legislative instruments and official sources were used in the preparation of Part 2 of this policy. They are listed by country in accordance with standard referencing practice for European-funded projects.

Greece

- Hellenic Republic (2018). Law 4577/2018 on the Security of Network and Information Systems. Government Gazette A' 199/03.12.2018. Available at: https://www.mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf
- Hellenic Republic (2019). Law 4624/2019 on the Protection of Natural Persons with Regard to the Processing of Personal Data (GDPR Implementation). Government Gazette A' 137/29.08.2019. Available at: https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF
- Hellenic Republic (2020). Law 4727/2020 on Digital Governance and Electronic Communications. Government Gazette A' 184/23.09.2020. Available at: https://adae.gov.gr/images/nomothetiko-plaisio/Nomos_4727_2020_01.pdf
- Hellenic Republic (2022). Law 4961/2022 on Emerging Technologies and Digital Governance. Government Gazette A' 146/27.07.2022. Available at: https://www.mindigital.gr/wp-content/uploads/2024/02/N-4961.pdf

- Hellenic Republic (2023). Law 5029/2023 on the Prevention and Management of School Violence and Cyberbullying. Government Gazette A' 55/10.03.2023. Available at: https://www.iep.edu.gr/wp-content/uploads/2025/01/2024-08-02_N_5029-2023.pdf
- Hellenic Republic (2024). Law 5160/2024 on Cybersecurity (NIS2 Transposition). Government Gazette A' 195/27.11.2024. Available at: https://search.et.gr/el/fek/?fekId=774154
- Ministry of Digital Governance, Hellenic Republic (2025). Ministerial Decision 1689/2025 on Cybersecurity Requirements for Public Sector Entities. Government Gazette B' 2186/06.05.2025. Available at: https://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf
- Ministry of Digital Governance, Hellenic Republic (2025). Ministerial Decision 1899/2025 on Information Security Governance for Public Entities. Government Gazette B' 4250/05.08.2025. Available at: https://cyber.gov.gr/wp-content/uploads/2025/03/KYA_APOFASI_10-Feb-2025_FEK-463_DEFTERO-TEFHOS.pdf

Italy

- Italian Republic (2003). Legislative Decree No. 196/2003 — Personal Data Protection Code, as amended by Legislative Decree No. 101/2018. Available at: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali.pdf
- Italian Republic (2021). Law No. 109/2021 converting Decree-Law No. 82/2021 — Establishment of the National Cybersecurity Agency (ACN). Gazzetta Ufficiale, 04.08.2021. Available at: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.codiceRedazionale=21A04841
- Italian Republic (2024). Legislative Decree No. 138/2024 — NIS2 Transposition. Gazzetta Ufficiale, 01.10.2024. Available at: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- Ministry of Education, Italian Republic (2020). Ministerial Decree No. 89/2020 — Guidelines for Digital Integrated Teaching (DDI). Available at: https://www.mim.gov.it/documents/20182/0/Decreto.pdf
- Ministry of Education, Italian Republic (2024). MIM Note No. 5274/2024 — Smartphone Use Restrictions in Schools. Available at: https://www.mim.gov.it/-/nota-n-5274-dell-11-luglio-2024
- Ministry of Education, Italian Republic (2025). MIM Circular No. 3392/2025 — Mobile Phone Restrictions in Schools. Available at: https://www.mim.gov.it/-/circolare-n-3392-del-16-giugno-2025
- Ministry of Education, Italian Republic (2025). Ministerial Decree No. 166/2025 — Guidelines for the Responsible Use of Artificial Intelligence in Schools. Available at: https://www.mim.gov.it/-/decreto-ministeriale-n-166-del-9-agosto-2025

Portugal

- Portuguese Republic (2018). Law No. 46/2018 — Legal Framework for Cyberspace Security (RFSC). Diário da República, 13.08.2018. Available at: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384
- Portuguese Republic (2019). Law No. 58/2019 — Portuguese Data Protection Law (GDPR Implementation). Diário da República, 08.08.2019. Available at: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982
- Council of Ministers, Portuguese Republic (2020). Resolution No. 30/2020 — Digital Transition Action Plan (PATD). Diário da República, 2020. Available at: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/30-2020-132133788
- Portuguese Republic (2025). Decree-Law No. 95/2025 — Prohibition of Smartphones in Schools (Years 1-6). Diário da República, 03.07.2025.

- Portuguese Republic (2025). Decree-Law No. 125/2025 — NIS2 Transposition (in force 3 April 2026). Diário da República, 04.12.2025. Available at: Decreto-Lei n.º 125/2025, de 4 de dezembro | DR
- Directorate-General of Education (DGE), Portugal. PADDE — School Digital Development Action Plan Framework. Available at: https://www.dge.mec.pt
- Centro Nacional de Cibersegurança (CNCS) / DGE, Portugal. SeguraNet — Digital Safety and Cybersecurity Resources for Schools. Available at: https://www.seguranet.pt
- Centro Nacional de Cibersegurança (CNCS), Portugal. CERT.PT — National Computer Emergency Response Team. Available at: https://www.cncs.gov.pt/pt/certpt/

Romania

- Romanian Republic (2018). Law No. 190/2018 — Personal Data Protection (GDPR Implementation). Official Gazette of Romania No. 651/26.07.2018. Available at: https://portal.just.ro/101/Documents/LEGE__190_2018_date_cu_caracter_personal.pdf
- Romanian Republic (2023). Law No. 58/2023 on Cybersecurity Obligations for Network and Information System Operators. Official Gazette of Romania No. 214/15.03.2023. Available at: https://legislatie.just.ro/Public/DetaliiDocument/265677
- Romanian Republic (2023). Law No. 198/2023 — Pre-university Education Law. Official Gazette of Romania No. 613/05.07.2023. Available at: https://edu.ro/sites/default/files/_fisiere/Minister/2023/Legi_educatie_Romania_educata/legi_monitor/Legea_invatamantului_preuniversitar_nr_198.pdf
- Government of Romania (2024). Emergency Ordinance (OUG) No. 155/2024 — NIS2 Transposition (approved by Law No. 124/2025). Official Gazette of Romania No. 1332/31.12.2024. Available at: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121
- Ministry of Education, Romania (2024). Order No. 5707/2024 — Student Statute. Official Gazette of Romania No. 795/12.08.2024. Available at: https://www.edu.ro/sites/default/files/_fisiere/Legislatie/2024/OM_5707_2024_Statut_elev.pdf
- Ministry of Education, Romania (2025). OMEC 6055-6058 — ROFUIP 2025-2026: Framework Regulation for the Organisation and Functioning of Pre-university Educational Units. Official Gazette of Romania No. 819/04.09.2025. Available at: https://www.edu.ro/ROFUIP

Slovakia

- Slovak Republic (2003). Act No. 596/2003 Coll. on State Administration in Education and School Self-Government (Schools and School Facilities Act), as amended. Available at: https://www.slov-lex.sk
- Slovak Republic (2008). Act No. 245/2008 Coll. on Education and Training (School Act), as amended by Act No. 323/2025 Coll. effective 1 January 2025 (mobile phone restrictions). Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2008/245/
- Slovak Republic (2018). Act No. 18/2018 Coll. on the Protection of Personal Data (GDPR Implementation). Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18/
- Slovak Republic (2018). Act No. 69/2018 Coll. on Cybersecurity. Available at: https://www.zakonypreludi.sk/zz/2018-69
- Slovak Republic (2024). Act No. 366/2024 Coll. on Cybersecurity (NIS2 Transposition), effective 1 January 2025. Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html

- Ministry of Education, Slovak Republic (2025). Guidance No. 1/2025 on the Prevention and Resolution of Cyberbullying in Schools and Educational Facilities. Available at: https://www.minedu.sk/data/att/d76/32441.fb1a83.pdf
- Ministry of Education, Slovak Republic (2025). Plan for the Responsible Use of Artificial Intelligence in Education 2025-2027. Available at: https://ai.iedu.sk/

ISO Standards

The following internationally recognised standards informed the development of the practical recommendations and governance measures presented in this Policy.

- International Organization for Standardization (ISO), ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Available at: https://www.iso.org/standard/27001
- International Organization for Standardization (ISO), ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection - Information security controls. Available at: https://www.iso.org/standard/75652.html
- International Organization for Standardization (ISO), ISO/IEC 27701:2025, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines. Available at: https://www.iso.org/standard/27701
- International Organization for Standardization (ISO), ISO 22301:2019, Security and resilience - Business continuity management systems - Requirements. Available at: https://www.iso.org/standard/75106.html
- International Organization for Standardization (ISO), ISO 31000:2018, Risk management - Guidelines. Available at: https://www.iso.org/standard/65694.html

Research and Evidence

The following research sources and publications were used in the preparation of Part 4 of this policy.

- European Commission (2025). Children's Voices on Cyberbullying: Consultation with Children Aged 12-17. Available at: https://eu-for-children.europa.eu/cyberbullying_en
- European Commission (2025). Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202505519
- European Commission / Better Internet for Kids (BIK+) / Insafe network (2025-2026). BIK Policy Monitor and Helpline Statistics. Available at: https://better-internet-for-kids.europa.eu/en
- European Union Agency for Cybersecurity (ENISA) (2022). Cybersecurity Education Initiatives in the EU Member States. Available at: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states
- OECD (2025). How's Life for Children in the Digital Age? Available at: https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en.html
- Polanin, J. R., Espelage, D. L., Grotpeter, J. K., et al. (2021). A Systematic Review and Meta-analysis of Interventions to Decrease Cyberbullying Perpetration and Victimization. Prevention Science. Available at: https://link.springer.com/article/10.1007/s11121-021-01259-y
- Torgal, C. and Aksoy, C. (2022). A Meta-Analysis of School-Based Cyberbullying Prevention Programs Impact on Cyber-Bystander Behavior. School Psychology Review, 52(2). Available at: https://www.tandfonline.com/doi/full/10.1080/2372966X.2021.1913037
- World Health Organization Regional Office for Europe (2024). Health Behaviour in School-aged Children (HBSC): Findings on Bullying and Cyberbullying. Available at: https://www.who.int/europe/initiatives/health-behaviour-in-school-aged-children-(hbsc)-study

- Cyberbullying and LGBTQ Youth: A Systematic Literature Review and Recommendations for Prevention and Intervention (2018). Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7163911/
- Correlations Between Social Media Addiction and Anxiety, Depression, FoMO, Loneliness and Self-Esteem Among Students: A Systematic Review and Meta-Analysis (2025). PLOS ONE. Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0329466