



ShieldNet

Document Title	ShieldNet Cybersecurity Standard – Education Add-on
Release Date	October 2025
Next Review	September 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	2.0

1. What is the Education Add-on

Education is a digitally transforming sector that faces unique cybersecurity challenges. Schools, universities, and training centers are increasingly targeted by cyberattacks - incidents can disrupt classes, expose student records, or even force institutions to shut down. Educational organizations handle very sensitive personal data – including information on minors – and must comply with strict laws on privacy and child protection (e.g. the EU General Data Protection Regulation for data protection, and national regulations on children’s data). The ShieldNet Education Add-on extends the core ShieldNet Cybersecurity Standard to address these sector-specific needs. ShieldNet’s core provides 48 plain-language controls as a baseline for all SMEs and nonprofits, designed to be modular for different industries. This Education Add-on builds on that foundation with additional controls tailored to research institutes, universities, K-12 schools, early childhood centers, and private training providers. The add-on retains ShieldNet’s practical, actionable style – each control is a concise “must-do” statement geared for small to medium organizations. By augmenting the core standard with education-specific safeguards, institutions can better protect student privacy, ensure continuity of learning, and meet education regulations. This need is underscored by new EU initiatives bringing more educational entities under cybersecurity laws – for example, the NIS2 Directive introduces stricter cyber risk management requirements for critical sectors including education institutions that manage sensitive data or provide essential services. In short, the Education Add-on provides a focused security playbook for the education sector’s unique risks and obligations, in harmony with ShieldNet’s mission to keep security manageable for smaller teams.

2. How to use the Education Add-on

The Education Add-on is meant to be adopted alongside the core ShieldNet controls, not as a standalone list. Educational organizations should first implement all relevant core controls (the baseline applicable to all sectors) and then augment them with the sector-specific controls from this add-on. Each institution should identify which category (or categories) below fit its profile - e.g. a research university would refer to section 3.2.1 Research Institutes & Universities, a public K-12 school to section 3.2.2 Primary/Secondary Schools, etc.. If an organization spans multiple categories (for instance, a university with an on-campus daycare, or a school district that also runs adult education classes), it should combine the applicable controls from each relevant section into its security program. The add-on's controls are grouped into the same five ShieldNet Action Zones – Know & Plan, Shield & Build, Watch & Patch, React & Recover, Learn & Lift - making it easy to slot these additional requirements into the existing framework.

ShieldNet follows a risk-based approach based on organization size and sector sensitivity. Education is considered a high-sensitivity sector – the confidentiality of student data (especially minors' data) and the continuity of teaching are critical. Thus, for any small or medium educational organization, these add-on controls should be treated as mandatory enhancements to the core controls (not optional). A micro-scale entity (e.g. a single-classroom daycare or small tutoring business) should still implement as many add-on controls as feasible based on risk – at minimum those addressing legal obligations (like protecting children's personal data) – even if some advanced measures must be scaled down due to limited capacity. Small and medium institutions (up to ~250 staff) are expected to implement the full set of relevant add-on controls; medium-sized ones should additionally prepare for potential audits or oversight on these sector-specific requirements (since regulators and authorities are increasingly scrutinizing cybersecurity in the education sector, especially where minors are involved). In practice, this means integrating the add-on controls into policies, procedures, and training. For example, a school district would update its incident response plan to include education-specific steps from this document (such as parent communication protocols), and a university IT department would incorporate these controls into its governance, procurement, and network management processes.

3. Action Zones

The controls in each category are organized by the five ShieldNet Action Zones to mirror the security lifecycle. Educational organizations should address all five zones for a comprehensive program:

- KNOW & PLAN - understanding assets, risks, and compliance obligations in the education context and planning accordingly.
- SHIELD & BUILD - implementing protective measures and secure infrastructure tailored to educational environments.
- WATCH & PATCH - monitoring systems for issues and keeping technology up-to-date against evolving threats.
- REACT & RECOVER - responding to incidents in a way that minimizes educational disruption and protects learners' safety.
- LEARN & LIFT - learning from incidents and changes to continuously improve and adapt to new cybersecurity challenges in education.

Each control below is written in plain language and is directly applicable. We reference EU regulations and standards (like GDPR, NIS2, etc.) where relevant to show alignment - adhering to these controls will help meet those legal requirements. Use this add-on as a checklist or extension of your core ShieldNet implementation: integrate the controls into your risk assessments, update your security policy to cover these items, and assign responsibility (IT staff, Info-Sec coordinator, administrators, teachers, etc.) for each. By following both the core and education-specific controls, even small institutions can achieve a level of security and compliance proportionate to the sensitivity of their work, while keeping the approach practical and scaled to their size.



3.1. COMMON CONTROLS

The Common Controls are the baseline cybersecurity requirements for all educational organizations in the ShieldNet program (research institutes, universities, K-12 schools, early childhood centers, and training providers). They extend the Core Standard with student-safety and data-protection specifics, organized under the five Action Zones. Each control is proportionate for small teams, written in plain English, and traceable to EU sources (e.g. GDPR, NIS2, child privacy directives). Implement these first, keep evidence lightweight but current (using simple checklists, policy documents, and logs), and you'll have a defensible, audit-ready baseline that protects students, safeguards personal data, and supports uninterrupted learning.

3.1.1. KNOW & PLAN

[KP-E1] Classify Student and Staff Data by Sensitivity

Control text: Create and maintain a short list of the personal data you handle for students, parents, and staff. Mark what is most sensitive, especially minors, health, and special needs data, then apply stronger protection such as restricted access and encryption.

Why: If you know what data you have and how sensitive it is, you can protect the most important records first and reduce accidental disclosure..

Evidence examples: Data inventory with sensitivity labels, data handling rules for sensitive records, access list showing restricted access, encryption settings for high sensitivity data.

Legal anchors: GDPR Art. 5(1)(c), GDPR Art. 5(1)(f), GDPR Art. 32, GDPR Recital 38.

[KP-E2] Assess and Manage Education-Specific Cyber Risks

Control text: At least once a year, and after major changes, identify education specific cyber risks such as ransomware, account takeover, and exam disruption. Record them in a simple risk register with an owner and due date, then review progress with leadership.

Why: A simple risk register helps you focus limited time and budget on what matters most and shows management oversight.

Evidence examples: Risk register with ratings, owners, and due dates, annual review notes, examples of completed actions such as MFA enabled or backups tested.

Legal anchors: NIS2 Art. 21(2)(a), GDPR Art. 32.

[KP-E3] Appoint a Data Protection Officer or Privacy Lead

Control text: Appoint a Data Protection Officer when GDPR requires it, or assign a privacy lead if not required. Give them authority to manage privacy tasks, coordinate breaches, and report to management.

Why: Clear ownership prevents privacy tasks from being missed and speeds up decision making during incidents.

Evidence examples: Appointment letter, role description, org chart, records of privacy reviews and advice to management, training record for the appointed person.

Legal anchors: GDPR Arts. 37–39, GDPR Arts. 33–34.

[KP-E4] Manage Parental Consent and Child Data Protection

Control text: Use a clear process to obtain and record parent or guardian consent where it is needed. Provide simple privacy information to children and parents, review tools and activities that process children's data, and run a DPIA for high risk cases.

Why: Children's data has extra protection. Clear consent and transparent notices reduce legal risk and build trust with parents.

Evidence examples: Consent forms and consent register, privacy notices for parents and students, DPIA reports for high risk tools, log of consent withdrawals and updates.

Legal anchors: GDPR Arts. 6-7, GDPR Art. 8(1), GDPR Arts. 12-14, GDPR Art. 35, GDPR Recital 38.

[KP-E5] AI Systems in Education — Inventory, Risk & Oversight

Control text: Keep an inventory of AI tools used for teaching, grading, admissions, or support. For each tool, record the purpose, data used, owner, and human oversight, and reassess risk after major updates or changes.

Why: AI can affect grades and access to education. Basic oversight reduces unfair outcomes, privacy issues, and compliance gaps.

Evidence examples: AI inventory with purpose, data, and owner, AI risk assessment notes, records of human review or override, user information notices, change log and approval for major updates.

Legal anchors: EU AI Act Arts. 9-15 where applicable, GDPR Art. 5, GDPR Art. 6, GDPR Art. 9, GDPR Art. 25, GDPR Art. 35.

3.1.2. SHIELD & BUILD

[SB-E1] Implement Secure Network Segmentation and Access Control

Control text: Separate your network into simple zones. At minimum use Staff and Admin, Students and Guests, and IoT and CCTV. Limit traffic between zones with firewall rules, use unique staff accounts, least privilege access, and MFA for admins and systems holding student data.

Why: Segmentation and strong access control keep problems in one area from reaching grades or student records.

Evidence examples: Network diagram showing VLAN or SSID separation, firewall rules summary, MFA enforcement evidence, list of staff and admin accounts, documented roles showing least privilege.

Legal anchors: NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(j), GDPR Art. 32, GDPR Art. 5(1)(f)..

[SB-E2] Maintain Secure and Updated Endpoints

Control text: Protect all school devices such as servers, staff laptops, and managed student devices with malware protection, a local firewall, screen lock, and automatic updates. Remove unsupported systems and keep an asset list with an owner and last update date.

Why: Most ransomware and data leaks start on unpatched or poorly protected devices. Basic endpoint hygiene gives strong protection with low effort.

Evidence examples: Asset list with last patch date, endpoint protection dashboard, update policy with patch deadlines, device management or patch reports, record of retired or replaced unsupported devices.

Legal anchors: NIS2 Art. 21(2)(e), NIS2 Art. 21(2)(i), GDPR Art. 32.

[SB-E3] Secure Configuration of Online Learning Platforms

Control text: Use only approved learning and video tools and set safe defaults such as meeting passwords, waiting rooms, and enrolled users only. Restrict screen sharing and recording, require MFA for staff, and store recordings and files in approved access controlled locations.

Why: Secure settings prevent class disruptions and reduce exposure of student data in online learning.

Evidence examples: List of approved platforms, screenshots of key security settings, role and permission list for the platform, audit logging enabled, storage location showing restricted access.

Legal anchors: GDPR Art. 25, GDPR Art. 32, NIS2 Art. 21(2)(h), NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(j).

[SB-E4] Protect CCTV and IoT Systems

Control text: Secure CCTV and IoT devices by changing default accounts, keeping firmware updated, and placing them on a separate network. Limit who can view or manage cameras, keep footage only as long as needed, display clear CCTV notices, and record consent when required.

Why: Cameras and IoT devices are common weak points. Good settings reduce privacy risk for children and staff.

Evidence examples: Camera and IoT inventory with firmware versions, proof default accounts changed, network segregation evidence, access list and viewing logs, retention settings and deletion proof, CCTV signage and consent records if used.

Legal anchors: GDPR Arts. 6-7, GDPR Art. 5(1)(e), GDPR Art. 5(1)(f), GDPR Art. 32.

3.1.3. WATCH & PATCH

[WP-E1] Continuous Monitoring and Logging

Control text: Collect security logs from key systems such as student information, learning platforms, email, and identity services, and review them on a defined schedule. Enable alerts for high risk events such as repeated failed logins, unusual access to student records, and admin changes, and assign someone to act on them.

Why: Early warning helps you react before a small issue becomes a major incident. Logs also provide evidence during investigations.

Evidence examples: Audit logging enabled for key services, alert reports or summary emails, log review checklist and schedule, tickets showing follow up on alerts, access logs for sensitive data.

Legal anchors: NIS2 Art. 21(2)(f), GDPR Art. 32, GDPR Art. 5(2).

[WP-E2] Manage Vulnerabilities and System Updates

Control text: Keep an up to date list of systems and software versions. Subscribe to vendor security alerts, run vulnerability scans on a schedule, and patch or mitigate critical issues quickly. Track what was fixed and when.

Why: Most attacks use known, already fixed weaknesses. Regular patching closes common entry points.

Evidence examples: Asset and version list, vulnerability scan reports, patch or mitigation log with dates, change tickets for urgent fixes, report showing patch compliance over time.

Legal anchors: NIS2 Art. 21(2)(e), GDPR Art. 32.

[WP-E3] Monitor and Secure Third-Party Services

Control text: Maintain a register of cloud and outsourced services. Turn on MFA and audit logs, review security settings, and make sure contracts require the provider to notify you quickly about incidents. Track vendor advisories and apply recommended configuration changes.

Why: A breach at a service provider can expose student data even if your own systems are secure. Basic vendor oversight reduces that risk.

Evidence examples: Third party services register, screenshots showing MFA and audit logging enabled, contract clauses for incident notification, evidence of periodic tenant security reviews, vendor advisories with documented follow up actions.

Legal anchors: NIS2 Art. 21(2)(d), GDPR Art. 28(1), GDPR Art. 28(3)(f), GDPR Arts. 33-34.

3.1.4. REACT & RECOVER

[RR-E1] Maintain an Education-Focused Incident Response Plan

Control text: Keep a short incident response plan with roles, contacts, containment steps, and communication for students, parents, staff, and authorities. Include simple playbooks for common cases such as ransomware, data leak, account takeover, and online harassment. Run at least one tabletop exercise per year and update the plan after lessons learned.

Why: A practiced plan reduces downtime and confusion and helps protect students and data during stressful events.

Evidence examples: Incident response plan and contact list, scenario playbooks, exercise records and lessons learned, change log showing updates, example incident ticket with actions taken.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 21(2)(c), GDPR Arts. 33-34.

[RR-E2] Maintain Secure Data Backup and Recovery Capability

Control text: Back up critical data and systems on a regular schedule. Keep at least one backup copy protected from deletion, such as offline or immutable storage. Restrict access to backups and test restores to confirm you can recover within your required time.

Why: Reliable backups are the fastest way to recover from ransomware, mistakes, or system failures without losing records.

Evidence examples: Backup schedule and policy, backup logs, proof of offline or immutable copy, restore test report, access list for backup storage.

Legal anchors: NIS2 Art. 21(2)(c), GDPR Art. 32(1)(c).

[RR-E3] Establish Alternate Learning Continuity Procedures

Control text: Prepare simple offline or manual procedures for teaching and student safety during IT outages, including attendance, essential student information, and parent communication. Keep printed rosters and emergency contacts available and run short downtime drills so staff know what to do.

Why: When systems are down, schools still need to operate safely and keep parents informed.

Evidence examples: Continuity plan section for IT downtime, printed offline kits such as rosters and forms, drill record, approved parent message templates, staff quick guide.

Legal anchors: NIS2 Art. 21(2)(c), GDPR Art. 32.

[RR-E4] Manage Breach Notification and Communication

Control text: Document how you assess and handle personal data breaches. When required, notify the Data Protection Authority within 72 hours and inform affected people in clear language. Use templates approved in advance, assign official spokespeople, and keep records of decisions and timelines.

Why: Fast, clear communication is required by GDPR and helps maintain trust during incidents.

Evidence examples: Breach procedure, Data Protection Authority contact list, notification templates, incident records showing assessment and timeline, communications log.

Legal anchors: GDPR Arts. 33–34.

3.1.5. LEARN & LIFT

[LL-E1] Provide Cybersecurity Awareness Training for Staff and Students

Control text: Train staff during onboarding and at least annually on phishing, safe passwords and MFA, protecting devices, handling student data, and how to report incidents. Provide age appropriate online safety lessons for students and reinforce with short reminders and quizzes.

Why: Most incidents start with human error. Regular, practical training reduces phishing success and improves reporting.

Evidence examples: Training materials, completion records, phishing simulation results if used, student lesson plans, reminder posters or emails.

Legal anchors: NIS2 Art. 21(2)(g), GDPR Art. 32, GDPR Art. 39(1)(b).

[LL-E2] Maintain a Security Audit and Continuous Improvement Cycle

Control text: At least annually, review whether your key security controls still work, including access control, backups, patching, and incident response. Document findings, assign owners, and track fixes to completion. After incidents, run a short lessons learned review and update processes.

Why: Routine Controls decay over time. Regular checkups catch gaps early and keep your program ready for audits.

Evidence examples: Self-assessment or audit report, remediation tracker with owners and dates, management review notes, lessons learned notes, updated policies and procedures.

Legal anchors: NIS2 Art. 21(2)(f), GDPR Art. 32(1)(d).

[LL-E3] Engage in Community and Information Sharing

Control text: Subscribe to trusted education sector cyber alerts such as national CERT, NREN, or ministry bulletins. Share anonymized lessons learned with peer organizations and use relevant advisories to update settings, training, or policies.

Why: Education organizations face similar attacks. Early warnings help small teams defend faster.

Evidence examples: Subscription records and received advisories, meeting notes or webinars attended, examples of updates made after an alert, membership in sector groups or forums.

Legal anchors: NIS2 Arts. 26-27, GDPR Recital 49.

3.2. CATEGORY-SPECIFIC CONTROLS

The Category-Specific Controls add focused requirements for particular educational contexts where risks and operations differ. These additional controls complement the Common Controls, drilling down on needs of four key categories: Research & Universities, Primary/Secondary Schools, Early Childhood (Daycares), and Private Training Providers. Start with the Common Controls, then layer on only the categories that match your scope. Each add-on narrows the “how” for your environment - e.g. securing research data and high-campus network usage in universities, protecting minors and online safety in K-12 schools, securing camera systems in daycares, or safeguarding course content and customer data in private training companies - while preserving the same format, evidence style, and legal mapping used throughout the standard.

3.2.1. *Research Institutes & Universities*

[KP-E6] Protect and Classify Research Data

Control text: Classify research data and store sensitive data only in approved locations with access control and encryption. If research uses personal data, define the lawful basis, minimize data, consider pseudonymization, and perform a DPIA when required. Obtain ethics approvals where applicable.

Why: Research data is valuable and often sensitive. Proportionate protection prevents loss of years of work and protects participants.

Evidence examples: Research data register and classification, data handling procedure, access list for sensitive repositories, encryption evidence, DPIA or consent documents, secure environment access logs.

Legal anchors: GDPR Art. 6, GDPR Art. 9, GDPR Art. 32, GDPR Art. 89, NIS2 Art. 21.

[SB-E5] Secure Campus Networks and Edgeless Computing Environment

Control text: Require authenticated access to campus networks such as eduroam or 802.1X. Segment networks for students, staff, research, and IoT, and control traffic between them. Protect the internet edge with filtering and intrusion detection where feasible. Restrict admin access to critical infrastructure with MFA and logging.

Why: Campus networks are open and heavily used. Authentication and segmentation reduce misuse and limit how far an attacker can move.

Evidence examples: : Wi Fi and wired authentication settings, network segmentation diagram and firewall rules, edge protection service proof, admin access controls, logs for admin actions.

Legal anchors: NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(j), GDPR Art. 32.

[WP-E4] Manage Academic Account Lifecycle and Access

Control text: Manage student and staff accounts through a join, move, leave process. Create accounts on time, change access when roles change, and disable accounts quickly when people leave. Require MFA for staff and admin accounts and review access at least each term. Limit or retire alumni accounts.

Why: Old accounts and excessive privileges are common entry points for attackers.

Evidence examples: Join, move, leave procedure, deprovisioning logs, MFA enforcement report, termly access review sign off, list of alumni accounts with reduced access.

Legal anchors: NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(j), GDPR Art. 32.

3.2.2. Primary & Secondary Schools

[KP-E7] Establish and Enforce an Acceptable Use Policy (AUP)

Control text: Create an Acceptable Use Policy for students and staff that sets clear rules for using school devices, accounts, and the internet. Include reporting steps for cyberbullying, online abuse, and suspicious messages. Communicate it in age appropriate language and collect acknowledgements each year from students and parents or guardians.

Why: Clear rules reduce risky behavior and help staff respond consistently to online safety issues.

Evidence examples: Acceptable Use Policy document, acknowledgements from students and parents, student online safety materials, description of the reporting channel, incident log entries linked to follow up actions.

Legal anchors: GDPR Recital 38, GDPR Art. 5(1)(f), GDPR Art. 32.

[SB-E6] Implement Web Content Filtering and Email Security

Control text: Use web filtering on student networks and devices to block harmful and malicious sites. Protect email with anti-spam and anti-phishing controls such as link and attachment scanning and quarantine. Provide a simple process to unblock legitimate educational resources when needed.

Why: Filtering reduces exposure to harmful content and blocks common phishing and malware attempts.

Evidence examples: Web filter settings and reports, unblock request log, email security settings, quarantine logs, examples of blocked phishing.

Legal anchors: GDPR Art. 32.

[WP-E5] Maintain Device and Lab Security Hygiene

Control text: Harden shared classroom and lab devices so changes reset between sessions using kiosk mode or restore on reboot. Regularly check for tampering and unauthorized software, keep a device inventory, and use device management where possible. Periodically scan for rogue devices such as unauthorized Wi Fi access points.

Why: Shared devices are often misused. Standard settings and quick reset reduce malware and misconfiguration risk.

Evidence examples: Lab device baseline settings, inspection checklist, device inventory or management compliance report, lost device tickets with lock or wipe proof, rogue device scan results.

Legal anchors: GDPR Art. 32, NIS2 Art. 21(2)(i).

[RR-E5] Integrate Child-Centric Incident Response Procedure

Control text: Extend your incident response plan to cover child safeguarding cases such as cyberbullying, harassment, sextortion, and exposure of minors' data. Define how IT, safeguarding staff, leadership, parents or guardians, and authorities coordinate. Prioritize student safety and privacy and preserve evidence safely.

Why: Many school incidents are about student welfare, not only IT. A coordinated response protects victims and prevents repeat harm.

Evidence examples: Incident response plan addendum for safeguarding cases, staff training records, contact list for local authorities or police, anonymized case notes, evidence handling guidance.

Legal anchors: GDPR Arts. 33-34 where personal data is involved, Directive 2011/93/EU where relevant.

[LL-E4] Strengthen Parental Engagement and Transparency

Control text: Share simple cyber safety guidance with parents or guardians through tips, short sessions, or newsletters. Publish a short yearly summary of key privacy and cybersecurity measures and improvements. Keep an easy way for parents to report concerns or incidents.

Why: Parents reinforce good habits at home. Transparent communication builds trust and improves early reporting.

Evidence examples: Parent newsletters or tip sheets, session agenda or slides, yearly summary, feedback log and follow up actions, parent survey results if used.

Legal anchors: GDPR Art. 12.

3.2.3. Early Childhood & Daycare

[SB-E7] Enforce Enhanced Security for Camera Monitoring Systems

Control text: Treat camera and baby monitor systems as high risk. Use vetted solutions with encryption, change default accounts, and require strong passwords and MFA if available. Keep cameras and recorders on a separate network and avoid direct internet exposure by using a VPN or secure relay. Limit retention and log who can view footage.

Why: Footage of young children is highly sensitive. Strong controls prevent external compromise and internal misuse.

Evidence examples: Camera system settings showing encryption and MFA, network segregation evidence, retention and auto delete settings, access log for viewing, firmware update log, CCTV notices and signage.

Legal anchors: GDPR Art. 5(1)(c), GDPR Art. 5(1)(e), GDPR Art. 5(1)(f), GDPR Art. 25, GDPR Art. 32.

[KP-E8] Ensure Child Data Privacy and GDPR Compliance

Control text: For daycare personal data such as enrolment details, health and allergy information, and photos, keep a Record of Processing Activities and perform DPIAs for high risk processing. Use consent for optional activities such as social media photos and document lawful bases for core operations. Provide short privacy information at enrolment, offer an easy way for parents to exercise rights, vet vendors and sign DPAs, and keep data in the EU or with equivalent safeguards.

Why: Daycares handle very sensitive data about vulnerable children. Good privacy governance reduces legal and reputational risk and supports parent trust.

Evidence examples: Record of Processing Activities, DPIA reports, consent records, parent privacy notice, DPAs with service providers, log of data rights requests and responses, evidence of EU hosting or safeguards.

Legal anchors: GDPR Art. 30, GDPR Art. 35, GDPR Arts. 6-7, GDPR Art. 9, GDPR Arts. 12-15, GDPR Art. 28.

[SB-E8] Enforce Secure Handling of Children's and Staff Devices

Control text: Control which devices are allowed in the daycare, including parent supplied devices. Approve only devices that are supported, updated, and not using default passwords. Configure children's tablets in restricted mode with only approved apps and minimal internet access. Do not

use staff personal phones for child data. For work phones, enforce encryption, screen lock, and remote wipe, and store photos only in approved systems.

Why: Uncontrolled devices can leak child data or bring malware into the network. Clear rules and secure settings keep handling safe by default.

Evidence examples: Device policy and acknowledgements, approved device checklist, screenshots of restricted profiles, inventory showing encryption and screen lock, remote wipe logs, incident records for removed non-compliant devices.

Legal anchors: GDPR Art. 25, GDPR Art. 32.

[RR-E6] Maintain Resilient Emergency Contact and Release Systems

Control text: Make sure emergency contacts and authorized child pick up lists are available during outages. Keep a secure printed copy and an encrypted offline copy. Update them when details change, limit access to trained staff, and run periodic drills.

Why: Even during IT outages, staff must safely release children only to authorized guardians.

Evidence examples: Emergency contact binder with review log, encrypted offline file with last sync date, drill record, staff acknowledgements or training, physical storage procedure such as locked cabinet and sign out.

Legal anchors: GDPR Art. 32.

3.2.4. Private Educational Centers

[KP-E9] Enforce Client Data Segregation and Protection

Control text: If you train multiple clients, keep each client's data and materials separate using separate tenants, folders, workspaces, or databases. Use per client access roles so one client cannot see another. Capture security and retention requirements in contracts and reflect them in system settings.

Why: Multi client environments are prone to accidental data mixing. Separation reduces privacy risk and protects client confidentiality and intellectual property.

Evidence examples: Access roles showing per client separation, tenant or workspace configuration, signed NDAs and DPAs, onboarding and offboarding checklist, audit logs showing correct access.

Legal anchors: GDPR Art. 5(1)(f), GDPR Art. 32, GDPR Art. 28, NIS2 Art. 21(2)(d) where applicable.

[SB-E9] Protect Intellectual Property and Course Content

Control text: Protect course materials from unauthorized sharing. Limit access to enrolled learners, use strong authentication, and disable public sharing links. Use watermarks or basic download controls where appropriate, and for live sessions use waiting rooms and verified participants. Set clear usage terms and a simple process to report and remove leaked content.

Why: Training content is often core intellectual property. Basic controls deter casual piracy and protect your business and reputation.

Evidence examples: Platform settings showing enrolment only access, examples of watermarked materials, learner terms shown before access, access expiry or deprovisioning evidence, takedown request log.

Legal anchors: Directive 2001/29/EC, Directive (EU) 2019/790, GDPR where personal data is included.

[WP-E6] Secure Payment Processing and Personal Information Handling

Control text: Use a PCI DSS compliant payment provider and use hosted checkout or tokenization, without storing card details in your systems. Protect enrolment and account data with HTTPS, strong authentication, and encryption for sensitive fields. Keep your website and plugins updated, run regular security checks, and monitor for fraud and suspicious activity.

Why: Public facing training portals are common targets. Outsourcing card processing and keeping the website secure reduces financial and privacy risk.

Evidence examples: Payment provider attestation, architecture showing hosted checkout or tokenization, website update log, vulnerability scan results and fixes, HTTPS check report, fraud monitoring alerts.

Legal anchors: GDPR Art. 32, Directive (EU) 2015/2366 (PSD2), PCI DSS contractual via payment provider.

[RR-E7] Communicate Incidents to Clients and Learners

Control text: Prepare a communication plan for incidents and outages that affect clients or learners. Define when and how you notify, who approves messages, and what guidance you provide such as password reset. Keep an alternative channel such as a status page or SMS list and test the process with exercises.

Why: Clear, timely updates preserve trust and help clients act quickly. It also supports GDPR notification duties.

Evidence examples: Client communication runbook with roles and timelines, message templates, client contact list, status page or alternative channel details, exercise record, contract clauses on notification.

Legal anchors: GDPR Arts. 33-34, GDPR Art. 28(3)(f).