International School of Tallinn

ICT & AI POLICY

Revised by the IST management, 20.04.2026

Approved by the Management Board of Tallinn International School OÜ, 21.04.2026

2026

Table of Content

Part I – Everyday ICT Use and Digital Conduct

Audience: Students; parents and guardians; teachers and staff

Purpose: Front-line rules, behavioural expectations, digital conduct, classroom use and AI guidance.

Policy 1: Acceptable Use Policy (AUP)

(ISO/IEC 27001 aligned, E-ITS aligned, IST operationally aligned; applies to staff, students, contractors)

Purpose

The purpose of this Acceptable Use Policy is to define appropriate, responsible, and secure use of IST's information systems, digital services, networks, and devices.

This policy ensures:
1. Safe and responsible technology use
2. Protection of IST's data and ICT systems
3. Compliance with ISO/IEC 27001:2022
4. Compliance with Estonian E-ITS baseline requirements
5. Compliance with EU AI Act and GDPR (General Data Protection Regulation)
5. Support for IST's educational mission

The AUP applies to all ICT resources provided or financed by IST.

Scope

This policy applies to:

Users

1. Staff
2. Teachers
3. Administrative personnel
4. Students
5. Contractors
6. Interns and temporary staff
7. Third-party vendors with access to IST systems

Systems

1. All IST-owned computers, laptops, tablets, phones
2. School network (wired and Wi-Fi including VLANs)
3. M365 environment (SharePoint, OneDrive, Teams, Exchange)
4. Toddle and other approved EdTech platforms
5. FortiGate and Aruba network systems
6. Telia Cloud services
7. Intune-managed devices
8. All other IST-managed or approved systems

Activities

All digital activities conducted using IST's ICT resources fall under this policy.

General Acceptable Use Requirements

Users must:

1. Use IST ICT resources **only** for educational, administrative, or authorized business purposes.
2. Comply with all IST ICT policies.
3. Report suspicious activity immediately.
4. Protect personal login credentials.
5. Access systems only with authorized accounts.
6. Only use approved software and tools.
7. Treat all devices and systems with care and follow digital hygiene best practices.

Prohibited Activities

Users are prohibited from engaging in:

Security Violations

1. Attempting to bypass authentication or security controls
2. Tampering with logs or security settings
3. Sharing passwords or MFA tokens
4. Using another user's account

Inappropriate or Illegal Use

1. Accessing or sharing violent, hateful, or inappropriate content
2. Engaging in harassment or bullying
3. Conducting unauthorized recordings of staff or students
4. Downloading or distributing copyrighted material illegally
5. Using IST systems for personal financial gain
6. Violating Estonian law or GDPR (General Data Protection Regulation)

Technical Misuse

1. Installing unauthorized software
2. Connecting personal access points or routers
3. Bypassing network configurations (e.g., VLAN restrictions)
4. Accessing restricted administrative systems
5. Attempting to disable antivirus, firewall, or logging systems

Use of IST-Owned Devices

Users must:

1. Use only their assigned device(s)
2. Always keep devices physically secure
3. Ensure devices are never left unattended in public spaces
4. Not remove security controls or Intune management (Microsoft system)
5. Ensure devices remain updated through Intune policies
6. Only install pre-approved software (via Company Portal if allowed for teachers)

Damage, loss, or theft must be reported immediately.

Use of BYOD Devices (Students & Staff)

BYOD (Bring Your Own Device) usage is permitted under the following rules:

1. BYOD devices may **never** access Restricted (Restricted Personal Data)
2. Access is limited to Internal and low-impact Confidential data
3. BYOD devices must be free of malware and have up-to-date OS patches
4. Users must not store IST data locally on BYOD devices
5. BYOD devices must not connect to restricted VLANs
6. If a BYOD device is suspected to be compromised, access may be blocked by ICT Governance or IT Administration

Acceptable BYOD access rules are further defined in the BYOD Policy.

Internet & Email Use

Internet

Permitted use includes:

1. Research
2. Communication
3. Educational content
4. Teacher/staff planning tasks
5. Administrative tasks

Prohibited use includes:

1. Gaming (unless approved for class)
2. Streaming entertainment media unrelated to education
3. Circumventing web filters
4. Accessing inappropriate or harmful content

Email

Users must:

1. Use IST email only for IST-related communication
2. Not send Confidential or Restricted data externally without proper justification
3. Not click suspicious links
4. Not forward IST emails to personal accounts
5. No mass mailings without permission

Data Protection Responsibilities

Users must:

1. Handle Restricted data with extreme care
2. Never store Restricted data outside approved M365 systems
3. Follow the Data Protection & Privacy Policy
4. Report accidental exposures immediately
5. Not photograph or share data displayed on screens unless authorized

Students must never access Restricted data under any circumstance.

Classroom and Learning Environments

Teachers must:

1. Supervise student digital activity during class
2. Ensure students access only approved applications
3. Report student misuse
4. Not use unapproved tools that process personal data

Students must:

1. Use devices only for class purposes during lessons
2. Not attempt to access teacher resources, grades, or restricted systems
3. Use respectful and appropriate digital communication

Communication Platforms

Allowed platforms:

1. Microsoft Teams
2. IST email
3. Approved EdTech tools

4. Any M365-integrated application approved by ICT Governance

Prohibited communication methods:

1. WhatsApp, Telegram, Messenger, or similar apps for discussing Restricted or Confidential information
2. Personal emails for school communication

Storage of IST Data

Users must store IST data **exclusively** in approved environments:

1. SharePoint
2. OneDrive
3. Microsoft Teams
4. IST approved EdTech and admin platforms

Users may not:

1. Store IST data on personal cloud services
2. Store data on USB drives unless encrypted and approved
3. Store data on BYOD devices
4. Use personal laptops to download data from SharePoint

Reporting Violations

All users must report violations to:

1. IT Administration – help@telia.ee (technical, security and access-related violations)
2. Data Protection Officer – dpo@ist.ee (privacy incidents, data protection matters)
3. Teachers (for student cases)

Student escalation path:

Homeroom Teacher → IB Coordinator → DPO (Data Protection Officer, dpo@ist.ee) /Director
Director determines whether parents must be informed.

Enforcement

Consequences depend on the nature of the violation.

Students

1. Verbal warning
2. Parent notification
3. Temporary loss of ICT privileges
4. Escalation to IB Coordinator or Director
5. Disciplinary action following school behaviour policies

Staff

1. Mandatory retraining
2. Written warning
3. Restriction of system access
4. Disciplinary procedures per employment regulations

Contractors & Vendors

1. Immediate revocation of access
2. Contract termination if necessary

Review Cycle

This policy must be reviewed:

1. Annually
2. When major ICT changes occur
3. In connection with risk assessment or incident findings

Policy 2: Bring Your Own Device (BYOD) Policy

(ISO 27001 aligned, E-ITS aligned, IST-specific, strict separation of BYOD from Restricted data access)

Purpose

The purpose of this BYOD Policy is to define how personal devices (laptops, tablets, phones) may be used to access IST ICT resources while protecting:

1. IST information assets
2. Student and staff privacy
3. Network security
4. Compliance with GDPR, ISO/IEC 27001:2022, and E-ITS

The policy ensures that personal devices do not introduce unnecessary security risks while supporting IST's digital learning environment.

Scope

This policy applies to:

Users

1. Students
2. Staff
3. Teachers
4. Interns
5. Contractors and vendors with temporary access

Devices

Any personally owned:

1. Laptops
2. Tablets
3. Smartphones
4. Wearable devices (smartwatches, where applicable)

Systems

BYOD access is limited to:

1. M365 web applications
2. Teams web/desktop apps (read-only for Restricted data)
3. Learning tools (Toddle, etc.)
4. Approved school resources that do **not** contain Restricted data

BYOD Access Rules

Permitted Access

BYOD devices may access:

1. IST email
2. Teams' meetings and chat
3. Class materials on SharePoint/Teams (Internal/Confidential)
4. Toddle and other EdTech systems
5. Internal-level data (not Confidential unless explicitly allowed)

Prohibited Access

BYOD devices are **strictly prohibited** from accessing:

1. Restricted (Restricted Personal Data)
2. HR systems

3. Confidential staff data
4. Administrator portals
5. Intune-administered profiles
6. M365 admin centre
7. Any system requiring privileged access

Prohibited Actions

Users may **not**:

1. Download IST data to personal devices
2. Sync OneDrive to a personal device
3. Store any Restricted or Confidential data on personal devices
4. Download student data, finance data, medical data, or Restricted internal records
5. Install unauthorized tools that connect to IST systems

BYOD Minimum Security Requirements

While BYOD devices are not required to meet full Intune compliance, they must meet the following minimum controls:

Device Security

1. Latest operating system updates installed
2. Working antivirus/anti-malware (where applicable)
3. Device not jailbroken or rooted
4. Screen lock enabled (PIN, biometrics, or password)
5. No unauthorized security tools or hacking utilities

Browser Requirements

1. Must use a modern, supported browser (Edge, Chrome, Safari, Firefox)
2. Browser updates must be applied regularly
3. Students and staff must not bypass browser security warnings

Network Restrictions

BYOD devices:

1. Must use the designated **Student** or **Staff** Wi-Fi VLAN
2. Must not connect to restricted VLANs (e.g., Admin, Devices, Building systems)
3. Must never activate personal hotspots to bypass filtering

Email & Communication

1. Only IST email may be used for IST-related communication
2. Email forwarding to personal accounts is prohibited
3. IST messages must not be stored in personal mailboxes

BYOD in Classrooms

Students

Students may use personal devices for:

1. Classwork
2. Research
3. Reading digital textbooks
4. Accessing approved learning platforms

Students may not:

1. Record staff or other students without consent
2. Use devices for gaming or entertainment during lessons
3. Access inappropriate content
4. Attempt to bypass filters or security controls

Teachers

Teachers may use BYOD devices for:

1. Displaying teaching materials (read-only)
2. Joining Teams classes
3. Light administrative communication

Teachers may not:

1. Download student records to personal devices
2. Access Restricted data from BYOD devices
3. Store lesson materials locally that contain student information

Loss, Theft, or Compromise of a BYOD Device

If a personal device used for IST purposes is:

1. Lost
2. Stolen
3. Infected with malware
4. Accessed by an unauthorized person
5. Suspected to be compromised

The user must immediately report the incident to:

1. IT Administration – help@telia.ee
2. ICT Governance – dpo@ist.ee
3. Homeroom teacher (for students, who will escalate)

Depending on severity, actions may include:

1. Forced password reset
2. Blocking access to IST systems
3. Required malware removal
4. Logging of incident per Incident Response Policy

Privacy Considerations

IST respects the privacy of personal devices.

IST will NOT:

1. Access personal files
2. Track personal device activities
3. Remotely wipe BYOD devices
4. Monitor non-IST usage
5. Install management profiles on BYOD devices

IST will:

1. Log access to IST systems from BYOD devices
2. Enforce Conditional Access restrictions
3. Block access to Restricted data
4. Require secure authentication (MFA for staff)

Responsibilities

Users

1. Maintain a secure device
2. Follow this policy and all IST ICT policies
3. Immediately report security concerns
4. Avoid storing IST data locally

Teachers

1. Supervise student use of BYOD in classes
2. Report misuse
3. Ensure students follow classroom digital rules

IT Administration

1. Configure Conditional Access to restrict BYOD appropriately
2. Block or limit access in case of security issues
3. Ensure data cannot be downloaded to personal devices
4. Support staff with MFA and access issues

ICT Governance

1. Oversee policy enforcement
2. Adjust controls based on risk assessments

Data Protection Officer (DPO)

1. Ensure BYOD access complies with GDPR
2. Investigate any privacy-related incidents

Enforcement

Violations of this policy may result in:

Students

1. Device confiscation during the school day
2. Loss of BYOD privileges
3. Escalation through Homeroom Teacher → IB Coordinator → Director
4. Disciplinary actions under school rules

Staff

1. Revocation of BYOD access rights
2. Written warnings or disciplinary measures
3. Mandatory security training

Contractors

1. Immediate revocation of access
2. Review of contractual obligations

Review Cycle

This policy must be reviewed:

1. Annually
2. Alongside the Access Control Policy
3. After security incidents involving personal devices
4. When new technologies (e.g., new Wi-Fi systems) are introduced

Policy 3: Artificial Intelligence (AI) Usage Policy

(*Aligned with GDPR, ISO/IEC 27001:2022, E-ITS, and IST Academic Integrity requirements*)

Purpose

The purpose of this policy is to define the secure, ethical, transparent, and age-appropriate use of Artificial Intelligence (AI) systems within the International School of Tallinn (IST).
This policy ensures that AI technologies:

1. Support learning and administrative efficiency
2. Protect minors and Restricted Personal Data
3. Comply with GDPR and Estonian legislation
4. Align with IST's Academic Integrity principles
5. Do not replace human responsibility or pedagogical judgment

AI must always support — never replace — professional accountability, safeguarding obligations, or student wellbeing.

Scope

This policy applies to:

1. All IST staff, teachers, administrators, and contractors
2. All students
3. All AI-enabled tools integrated into or used alongside IST systems
4. All AI systems used within Microsoft 365 (including Copilot)
5. Any external AI services accessed using IST devices or accounts

This policy must be read in conjunction with:

1. Data Protection & Privacy Policy
2. ICT Acceptable Use Policy
3. BYOD Policy
4. Access Control Policy
5. Logging & Monitoring Policy
6. Incident Response Plan

Definitions

For this policy:
1. Artificial Intelligence (AI) refers to systems capable of generating, analysing, or transforming content using machine learning or automated decision logic.
2. Generative AI refers to tools capable of creating text, images, code, audio, or other content (e.g., large language models).
3. Restricted Data refers to GDPR special-category personal data, including medical, dietary, religious, financial, assessments or SEN-related information concerning minors.

Core Principles

AI use at IST must always be:

- Age-appropriate
- Transparent
- Secure
- Ethical
- Accountable
- Human-supervised

AI outputs are advisory in nature. Final responsibility always remains with the human user.

AI systems must never make autonomous decisions affecting:

1. Student academic evaluation
2. Student safeguarding
3. Medical considerations
4. Disciplinary decisions
5. HR decisions

Age Classification & Access Control (Microsoft 365)

IST uses Microsoft 365 age classifications:

1. Minor – younger students (12 years old and under)
2. Not Adult – older minor students (13-17 years old)
3. Adult – staff and management (at least18 years old)

AI access and functionality may differ depending on classification.

Students may only use AI tools:

1. Approved by IST
2. Supervised by teachers (younger cohorts)
3. Within defined educational boundaries

Administrative AI access must follow role-based access control under the Access Control Policy.

AI Use by Students

AI may be used as a learning support tool, not as a replacement for original work.
Permitted uses include:

1. Concept clarification
2. Idea generation
3. Language support
4. Structured revision assistance
5. Programming guidance (older cohorts)

Prohibited uses include:

1. Submitting AI-generated work as original assessed work
2. Using AI to conceal plagiarism
3. Impersonating staff or students
4. Creating manipulated, deceptive, or harmful content
5. Generating deepfake media
6. Producing misinformation intentionally

Older students (NotAdult classification) must disclose AI usage in assessed work in accordance with IST Academic Integrity requirements.
Younger students must use AI only under guided supervision.

AI Use by Teachers

Teachers may use AI to support:

1. Lesson planning
2. Differentiated instruction
3. Administrative drafting
4. Content adaptation
5. Professional reflection

However:

1. AI-generated materials must be reviewed for accuracy
2. Pedagogical judgment cannot be delegated to AI
3. Teachers remain responsible for grading decisions
4. AI must not independently generate report card evaluations without human validation

When AI materially influences student assessment or feedback, transparency must be maintained.

AI use by Administrative & Management

Administrative AI use is permitted only for work-related tasks and must comply with:

1. Data Protection & Privacy Policy
2. Supplier & Third-Party Management Policy

Preferred AI systems:

1. Microsoft 365 Copilot
2. IST-managed AI environments

Strictly prohibited:

1. Uploading student data into public AI platforms
2. Uploading Restricted data into any external AI system
3. Processing HR, medical, safeguarding, or financial data via public AI tools
4. Copying internal documents into non-approved AI services

No Restricted data may be processed by AI systems unless explicitly approved by the DPO and ICT Governance and supported by contractual safeguards.

Restricted Data & Safeguarding

Under no circumstances may AI systems process:

1. Personal/ private data
2. Medical data
3. SEN records
4. Dietary or allergy records
5. Religious data
6. Financial data linked to an identifiable individual

AI must not be used for behavioural prediction, profiling of minors, or automated risk scoring.
Safeguarding decisions must remain entirely human-led.

Transparency & Disclosure

AI use must be transparent when it affects:

1. Student submissions
2. Assessment outcomes
3. Official communications
4. Policy drafting
5. Decision-making processes

Where appropriate, users must disclose AI assistance.
Failure to disclose AI use in assessed work may be treated under Academic Integrity procedures.

Logging, Monitoring & Risk Management

AI usage within IST systems may be logged according to the Logging & Monitoring Policy.
High-risk AI activities may trigger review under:

1. Risk Management Policy
2. Incident Response Plan

If AI misuse results in potential data exposure, it must be reported immediately under the Incident Response Plan.

Third-Party AI Providers

All AI vendors must:

1. Undergo supplier risk assessment
2. Provide GDPR-compliant DPAs (Data Processing Agreements)
3. Disclose sub-processors
4. Confirm EU data residency (where applicable)

New AI systems must be reviewed for data protection compliance.

Violations

Violations of this policy may result in:

Students:

1. Academic integrity review
2. Loss of ICT privileges
3. Disciplinary action

Staff:

1. Mandatory retraining
2. Access restrictions
3. Disciplinary procedures

Vendors:

1. Immediate access revocation
2. Contract review or termination

Severe misuse involving personal data may trigger GDPR breach procedures.

Review Cycle

This policy must be reviewed:

1. Annually
2. After major AI system adoption
3. After regulatory changes (EU AI Act implications)
4. Following AI-related incidents

IST TECHNOLOGY USE RULES AND GUIDELINES

For Students

Be Safe

1. Use your **own** IST account — never use someone else's.
2. Keep your password private.
3. If something feels strange (pop-ups, weird links, unexpected login requests), **tell a teacher immediately**.

Be Responsible

1. Use devices and the internet **for learning**, not for games or entertainment during lessons.
2. Treat all school devices with care — keep drinks away, carry them safely, and report damage right away.
3. Only use apps and websites that your teacher or IST has approved.

Be Respectful

1. Never take photos, videos, or recordings of other students or teachers without permission.
2. Communicate politely online — Teams chats and messages must follow school rules.
3. Do not access materials, folders, or systems meant for teachers or staff.

Keep Information Private

1. Never download or save school files to your personal device.
2. Do not share personal information (yours or others') outside school systems.
3. Do not use personal messaging apps (WhatsApp, Messenger, Instagram, etc.) for school communication.

Use Devices Correctly

1. Connect only to the **Student Wi-Fi** network.
2. Do not try to bypass filters, blocks, or security settings.
3. Do not install apps or software on school devices unless approved.
4. Keep personal devices updated and free of malware if you use them for school.

Follow Classroom Expectations

1. Use devices only when your teacher says it's allowed.
2. Close all unrelated tabs or apps during class.
3. Follow your teacher's instructions for online tools, tests, and assignments.

Report Problems Quickly

Tell your **teacher**, **homeroom teacher**, or **IT support** immediately if:

1. Your device is lost or damaged
2. You think someone else used your account
3. You see inappropriate content
4. You receive suspicious messages
5. Something doesn't work correctly

Reporting helps protect **you**, your classmates, and the school.

Remember

Using technology at IST is a privilege.
Using it safely and responsibly helps everyone learn better.

For Parents / Guardians

Dear Parents and Guardians - To support safe and effective learning, all students at IST follow a set of essential expectations when using school technology, devices, and online platforms. Please review these key points so you know how we work together to keep students safe and responsible online.

Student Safety Online

We teach students to:

1. Use only their **own** IST account
2. Keep passwords private and secure
3. Report suspicious links, pop-ups, or unusual login requests immediately

If a device is lost, damaged, or compromised, students must tell a teacher or ICT staff right away.

Appropriate Use of Devices

Students are expected to:

1. Use technology for **learning**, not entertainment during class
2. Handle school devices responsibly
3. Use only school-approved apps, websites, and tools

Teachers supervise classroom use, but we rely on families reinforcing proper behaviour at home.

Respectful Digital Conduct

IST expects students to:

1. Communicate politely in Teams and online platforms
2. Avoid recording or photographing others without permission
3. Never attempt to access staff files, systems, or restricted areas

We follow a clear escalation process - **Homeroom Teacher → Programme Coordinator → Director / DPO.**

Protecting Personal Information

To ensure privacy and GDPR compliance:

1. Students must not download school files onto personal devices
2. Personal messaging apps (WhatsApp, Facebook Messenger, etc.) must not be used for school communication
3. Restricted information is handled only through IST's secure Microsoft 365 systems

You can support this at home by reminding students not to share private information online.

Use of Personal Devices (BYOD)

Students may bring personal devices for learning, but:

1. They must connect only to the **Student Wi-Fi**
2. Devices must be updated and free of malware
3. Personal devices may **not** access Restricted student records or restricted school systems

IST staff can temporarily block access if a personal device poses a security risk.

Communication and Support

If your child experiences technical issues, inappropriate online behaviour, or device-related problems, please encourage them to report it immediately.
Early reporting helps protect your child, their classmates, and the school.
Parents may contact IST IT Support or the homeroom teacher for any concerns.

Working together

Be reinforcing these guidelines **at home**, you help us create a safe, respectful, and modern digital learning environment for all IST students. Your support is essential. If you have questions, contact us.

For staff and teachers

This page summarizes the key ICT rules every teacher must follow to protect student data, maintain system security, and support smooth daily operations.

Accounts, Passwords & MFA

1. Use only your assigned IST account.
2. Never share your password or MFA code with anyone — not even IT Administration.
3. Always use MFA.
4. Password changes are required **only** when suspicious activity occurs.
5. Report unexpected MFA prompts immediately — this may indicate account compromise.

Handling Student Data

You are responsible for protecting all information you handle.

1. **Never download** student files to personal devices.
2. **Do not store** student data outside Microsoft 365.
3. BYOD devices **cannot** be used for viewing or storing Restricted student data (medical, dietary, religious, financial, SEN info).
4. Only use school-approved apps and platforms for teaching and communication.
5. Report any data exposure or accidental access immediately.

Using Devices

1. All IST laptops must remain enrolled in **Intune**.
2. Do not remove security settings, antivirus, or updates.
3. Install only apps available in the **Company Portal** or approved by ICT.
4. Keep the device physically secure; report loss/theft right away.
5. Close or lock your device when leaving it unattended.

Classroom Technology Expectations

1. Supervise student device use during lessons.
2. Ensure students stay on learning tasks and follow AUP rules.
3. Do not use personal messaging tools (WhatsApp, Messenger, etc.) for school matters.
4. Only record, photograph, or share student materials if permitted / aligned with IST policies.
5. Immediately report any inappropriate online behaviour.

Email, Teams & Communication

1. Use IST email and Teams for all school-related communication.
2. Avoid sending Confidential or Restricted data externally unless necessary.
3. Never forward school email to personal accounts.
4. Keep Teams channels organized; avoid creating unnecessary groups or chats.

Wi-Fi & Network Use

1. Connect only to the **Teacher Wi-Fi**.
2. Do not attempt to modify or bypass network configurations.
3. Report unusual network delays, blocked websites, or connectivity issues to IT Support.

Change Requests & ICT Support

1. Any change to systems, permissions, or teaching platforms must follow the **Change Management** process.
2. Submit ICT support tickets through Telia's ticketing system for all issues.
3. For urgent problems, escalate through ICT Governance. dpo@ist.ee

Incident Reporting

Immediately report:

1. Lost or stolen devices
2. Unusual login attempts or MFA prompts
3. Suspicious emails
4. Inappropriate student behaviour online
5. Accidental sharing of files
6. Any activity that “does not look right”

Fast reporting helps prevent bigger issues.

Professional Conduct Online

1. Model safe and respectful digital behaviour for students.
2. Keep communication professional across all IST platforms.
3. Avoid accessing IST systems on unsecured public Wi-Fi.

By following these rules, you help keep our school’s digital environment safe, compliant and effective for learning and teaching.

1. Part II – Data Protection and Privacy

Audience: Parents and guardians; DPO; management; staff handling personal data
Purpose: ICT-related privacy safeguards, technical handling expectations and retention structure.

Policy 4: Data Protection & Privacy Policy

This topic is governed primarily by the separate IST Data Protection Policy. Within this ICT Policy Suite, Part II acts as the ICT-facing bridge section and should be read together with the separate data protection document where parent-facing privacy information is required.

This Part focuses on the ICT and operational implications of data protection, including technical safeguards, data handling expectations, access restrictions, retention expectations, and cross-references to related controls elsewhere in the suite.

The most relevant linked controls remain the Access Control Policy, Logging & Monitoring Policy, Incident Response Plan, Supplier & Third-Party Management Policy, and the Acceptable Use and BYOD rules where personal data is handled through school systems.

The retention schedule below remains part of this suite and supports the operational implementation of privacy, accountability, and deletion expectations.

ANNEX: Data Retention Schedule

Below is the full, production-grade version, aligned with IST Risk Management Policy.

Data Category	Retention Period	Notes / Legal Basis	Storage Location
Student Personal Data	Until leave + 2 years	Administrative necessity	M365 (SharePoint/OneDrive), Directo
Student Academic Records	Indefinite	Common best practices Estonian regulations	M365, Toddle
Restricted Student Data (medical, dietary, religious, special needs)	Only while needed; must be deleted immediately when no longer relevant	GDPR Art. 5(1)(e)	M365 Restricted SharePoint libraries
Parent / Guardian Contact Data Applicants Data (not joined)	Until leave + 2 years Application period + 1 year	Administrative need	M365, Directo
Staff HR Records	Employment period + 7 years	Estonian labour law & HR best practice	M365 HR site, Directo
Payroll/Financial Records	7 years	Estonian accounting law	M365 / Accounting systems (Directo)
Incident Reports	5 years	GDPR accountability, E-ITS	M365 IR library
Data Breach Logs	5 years	GDPR Art. 33 and 34 documentation	DPO-controlled storage
Access Logs (Azure AD)	Default 30 days	Licensing limitation	Microsoft cloud
M365 Unified Audit Log	Default 90 days	Licensing limitation	Microsoft cloud
Firewall Logs (FortiGate)	30 days	Telia retention commitment	Telia-managed
Intune Device Logs	Default retention	Microsoft cloud	
System Backups (Veeam)	30–90 days	Per Telia Cloud configuration	Telia Cloud
Email	Default M365 retention; purge on account deprovision	Operational practice	Exchange Online
IT Change Records	3 years	ISO 27001 audit trail	Change Register
Supplier Contracts & DPAs	Duration of contract + 3 years	GDPR & ISO 27001	Supplier Library