International School of Tallinn

DATA PROTECTION POLICY

TABLE OF CONTENT

1. Purpose and Scope

The International School of Tallinn (IST) is committed to protecting the privacy and personal data of its community in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR), the Estonian Personal Data Protection Act (IKS), and applicable education, employment, safeguarding, and financial legislation.

This Policy explains how IST collects, processes, stores, shares, and protects personal data relating to students, parents or guardians, staff members, applicants, alumni, contractors, visitors, and website users.

This Policy applies to all personal data processed by IST, regardless of format (digital or physical) and regardless of storage location.

This Policy complements the publicly available Privacy Policy published on https://ist.ee/

2. Legal Framework:

- The General Data Protection Regulation (GDPR)
- The Estonian Personal Data Protection Act (IKS)
- The Estonian Education Act and related regulations
- The Employment Contracts Act
- The Accounting Act
- The ePrivacy Directive
- Guidance issued by the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)

3. Definitions and Abbreviations

Personal Data – Any information relating to an identified or identifiable natural person.

Special Categories of Personal Data – Data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a natural person's sex life or sexual orientation.

Controller – The entity determining the purposes and means of processing personal data. IST acts as the Controller.

Processor – A third party processing personal data on behalf of IST.

DPO (Data Protection Officer) – The individual appointed by IST to oversee compliance with data protection legislation.

ICT (Information and Communication Technology) – The digital systems, software, devices, networks, and communication platforms used by IST to process, store, transmit, and secure personal data. This includes cloud services, identity management systems, learning platforms, and managed devices.

EHIS (Estonian Education Information System) – The national education database managed by Estonian authorities.

CCTV (Closed-Circuit Television) – A video surveillance system used to monitor specific areas of school premises for safety and security purposes. CCTV systems at IST do not record audio.

LIA (Legitimate Interest Assessment) – A documented assessment to ensure processing based on legitimate interest is lawful and proportionate.

DPIA (Data Protection Impact Assessment) – A structured assessment conducted where processing may result in high risk to individuals' rights and freedoms.

SCC (Standard Contractual Clauses) – European Commission-approved contractual clauses safeguarding international data transfers.

EU/EEA – European Union and European Economic Area.

Restricted Data – Personal data classified by IST as requiring enhanced protection.

MFA (Multi-Factor Authentication) – A security mechanism requiring more than one verification factor for access.

AI (Artificial Intelligence) – Technology capable of performing tasks typically requiring human intelligence.

4. Data Protection Principles

IST processes personal data according to the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability.

5. Lawful Basis for Processing

IST processes personal data under:

5.1 Contract

Where processing is necessary for schooling agreements, employment contracts, or service agreements.

5.2 Legal Obligation

Where processing is required by law, including reporting to EHIS, compliance with accounting and employment regulations, and safeguarding obligations.

5.3 Legitimate Interest

Where processing is necessary to ensure campus safety, IT security, fraud prevention, and operational continuity. Legitimate Interest Assessments are conducted where appropriate.

5.4 Consent

Where required for marketing communications, public image publication, or optional services.

5.5 Special Categories

Processed only where legally permitted, including for health services, SEN support, safeguarding, occupational health, or legal claims.

6. Categories of Personal Data

IST processes personal data relating to:

- Students (academic, behavioural, health, safeguarding, dietary and meal administration data)
- Parents or guardians (contact and financial data)
- Staff (employment and payroll records)
- Applicants (application and recruitment data)
- Visitors (visitor logs and CCTV recordings)

7. Children's Data Protection

IST recognises the enhanced protection required for children's data.

Processing is primarily based on contractual necessity and legal obligation. Parental consent is required for marketing and public image publication.

IST does not use automated decision-making or profiling that produces legal or similarly significant effects concerning students.

Artificial Intelligence systems are not used for admission decisions, academic grading, or disciplinary actions without meaningful human oversight.

8. Information and Communication Technology (ICT) and Technical Safeguards

IST operates primarily within a Microsoft 365 A3 Education environment.

Microsoft 365 services used by IST are hosted within the European Union.

Core systems include Exchange, SharePoint, Teams, OneDrive, Entra ID, Intune, and EU-hosted backup solutions.

Access is controlled through:

- Mandatory Multi-Factor Authentication
- Role-Based Access Control
- Conditional Access policies
- Logging and monitoring

Data is encrypted in transit and at rest. Managed devices are encrypted and monitored for compliance.

Restricted Data may not be accessed via unmanaged personal devices. Where international access occurs, appropriate safeguards such as Standard Contractual Clauses are applied.

Detailed authentication, account provisioning, and password management requirements are defined in the IST ICT Security Policy.

Access rights are reviewed periodically to ensure ongoing compliance with the principle of least privilege.

9. Learning Management System (Toddle)

IST uses Toddle as its Learning Management System for curriculum management, student assessment, communication between teachers and families, and documentation of learning progress.

The system may contain academic records, assessment data, attendance information, teacher feedback, and communication records.

Access is role-based and limited according to organisational responsibilities:

- Students access only their assigned classes.
- Teachers access only their assigned instructional areas.
- Parents or guardians are granted access to their child's educational information in accordance with parental responsibility and contractual arrangements.
- Administrative access is restricted to authorised roles.

Where AI-supported features within Toddle are used, they operate under human supervision and in accordance with the IST AI Policy.

Where international transfers occur, appropriate safeguards, including Standard Contractual Clauses, are implemented.

10. Third-Party Processors

IST engages approved third-party processors grouped by function as follows:

Category	Examples	Purpose of Processing
Core Cloud & Infrastructure	Microsoft, Google Workspace (where applicable), Dropbox	Email services, document storage, collaboration, identity management
Learning Platforms	Toddle	Curriculum management, assessment, learning documentation
National Education Systems	EHIS, ARNO	Legal reporting and student administration
Finance & Payment Services	Directo, EveryPay	Accounting, payroll, tuition fee processing
Recruitment Services	MoveMyTalent	Staff recruitment and candidate management
Examination & Accreditation Bodies	IB Organization and similar bodies	Assessment administration and certification

Category	Examples	Purpose of Processing
Educational Transfers	Universities and receiving institutions	Student transcripts and recommendation documentation
Communication & Marketing	MailerLite, Meta platforms	Newsletters and community engagement
Website & Consent Management	Wordpress, CookieYes	Website compliance and cookie consent management
Educational & Design Tools	Canva	Educational content creation
Health & Student Support	Healthcare providers, external specialists	School health and student support services
Extracurricular & Field Trip Providers	Approved activity providers and visit venues	Organisation of school activities and educational visits
Professional Services	Legal, accounting, training providers	Advisory and operational support
Insurance Providers	Approved insurance partners (where applicable)	Insurance administration in case of incident
Media & Content Services	External photographers and videographers	Documentation of school events

Where processors act as independent controllers (for example, certain examination bodies or universities), data sharing occurs in accordance with legal and contractual requirements.

This list is non-exhaustive. A complete and regularly updated processor register is maintained internally by IST.

Vendor risk assessments evaluate data sensitivity, international transfer risks, technical safeguards, contractual protections, and proportionality before approval.

All processors are required to enter into Data Processing Agreements and implement appropriate safeguards in accordance with GDPR.

11. INTERNATIONAL TRANSFERS

Where personal data is transferred outside the European Union (EU) or European Economic Area (EEA), IST ensures that appropriate safeguards are in place in accordance with GDPR requirements.

Such safeguards may include:

- Reliance on European Commission adequacy decisions;
- The use of Standard Contractual Clauses (SCC);
- Transfer Risk Assessments evaluating the legal environment of the receiving country;

- Implementation of supplementary technical or organisational safeguards where necessary.

International transfers may occur, for example, in connection with cloud service providers, examination and accreditation bodies, international university applications, or other approved service providers operating outside the EU/EEA.

IST ensures that all such transfers are assessed and documented in accordance with applicable data protection legislation.

12. Data Retention

IST retains personal data only for as long as necessary to fulfil the purposes for which it was collected and in accordance with the storage limitation principle under GDPR.

Retention periods are determined based on:

- Legal obligations under Estonian and European Union law;
- Contractual requirements;
- Safeguarding considerations;
- Limitation periods for potential legal claims;
- Educational record-keeping requirements.

A detailed Retention Schedule is maintained internally and approved by school management.

As a general principle:

- Student academic records may be retained for long-term archival purposes in order to verify educational history, certification, and compliance with regulatory requirements.
- Employment and payroll records are retained in accordance with applicable labour legislation, including statutory retention requirements.
- Financial and accounting records are retained in accordance with statutory accounting obligations.
- Recruitment data for unsuccessful applicants is retained until the end of the recruitment process and may be retained for up to one additional year where the candidate has provided explicit consent.
- Access logs and system records are retained only as long as necessary for security monitoring and system integrity.
- CCTV recordings are retained for 30 days unless required for investigation of a specific incident.

Where retention is based on legal obligation, such periods may extend beyond the termination of the contractual relationship.

Where personal data is no longer required, it is securely deleted, destroyed, or anonymised in accordance with approved procedures.

13. Data Subject Rights

Individuals have the right to access, rectify, erase, restrict, object, request portability, withdraw consent, and not be subject to automated decision-making. Subject to applicable legal limitations.

Individuals have the right to lodge a complaint with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon).

Requests must be submitted to dpo@ist.ee and are generally fulfilled within one month.

14. Staff Responsibilities

All staff members are responsible for protecting personal data in accordance with this Policy and applicable legislation.

Staff must:

- Process personal data securely and confidentially;
- Access personal data only where necessary for their professional duties ("need-to-know" principle);
- Avoid unauthorised disclosure, whether verbal, written, or digital;
- Follow approved data retention and secure disposal procedures;
- Use only authorised systems and devices for processing personal data;
- Immediately report suspected or actual personal data breaches;
- Participate in required data protection and safeguarding training;
- Seek guidance from the Data Protection Officer where uncertainty exists.

Confidentiality obligations continue after the termination of employment or any contractual relationship.

Failure to comply with this Policy may result in disciplinary action in accordance with IST procedures.

15. Closed-Circuit Television (CCTV)

IST uses Closed-Circuit Television (CCTV) systems to support the safety and security of students, staff, visitors, and school property.

CCTV cameras are installed in selected indoor and outdoor areas of the school premises. They monitor general areas such as corridors, entrances, and outdoor spaces. Cameras are not used to monitor specific individuals and do not record audio.

Recordings are accessed only when necessary, for example in the case of a safety concern, incident investigation, or suspected damage to property. Access to CCTV recordings is strictly limited to authorised personnel.

CCTV recordings are retained for 30 days and are automatically deleted thereafter, unless a recording is required for the investigation of a specific incident.

Recordings may be disclosed to law enforcement authorities where legally required.

Clear signage informs individuals about the presence of CCTV on school premises.

16. Marketing and Communications

IST communicates with its community and prospective families through newsletters, website content, social media platforms, and admission-related communications.

Email newsletters are distributed using MailerLite. Electronic marketing communications are sent only where valid consent has been obtained or where lawful "soft opt-in" applies in accordance with applicable legislation. All marketing communications include a clear unsubscribe mechanism.

Suppression lists are maintained to ensure that individuals who opt out of communications are not contacted for marketing purposes.

The IST website uses CookieYes to manage cookie consent. Users may review and adjust their cookie preferences through the consent banner available on the website.

IST may use social media platforms, including Meta platforms, for community engagement and promotional activities. Where targeted advertising tools are used, such processing is carried out in accordance with applicable data protection and electronic communications laws and subject to user consent where required.

Website inquiry and contact forms are currently processed within the website administration environment and transmitted to authorised school staff for response. IST is committed to processing such inquiries within secure systems and is implementing measures to further align admission inquiry handling with its Microsoft 365 environment hosted within the European Union.

Photographs and video materials used for promotional purposes are published only where appropriate consent has been obtained. This applies to website publications, newsletters, and social media platforms.

Event registrations and internal community communications are primarily managed through secure Microsoft-based systems.

The IST website may include chatbot functionality designed to assist users with general information. Users are advised not to submit sensitive or personal data through chatbot interfaces. Submission of personal data through such tools remains the responsibility of the user.

Consent for marketing communications may be withdrawn at any time.

Marketing communications are directed to parents, guardians, alumni, and adult community members. IST does not conduct direct marketing targeted at children.

17. Artificial Intelligence

IST may use Artificial Intelligence (AI) tools in accordance with its separate AI Policy and applicable data protection legislation.

AI tools may be used to support administrative efficiency, educational processes, communication, and data analysis. Such tools are implemented in a manner that respects privacy, safeguards personal data, and ensures appropriate human oversight.

Restricted Data must not be entered into publicly accessible AI systems without formal approval and documented safeguards.

AI systems are not used for admission decisions, academic grading, or disciplinary actions without meaningful human review.

Where AI-supported features are integrated within approved platforms (such as learning systems), their use remains subject to role-based access controls and supervision by authorised staff.

IST monitors developments in European Union AI regulation and adapts its practices accordingly.

18. Governance and Accountability

IST demonstrates compliance through:

- Appointment of a Data Protection Officer
- Maintenance of a Register of Processing Activities
- Conducting Data Protection Impact Assessments
- Conducting Legitimate Interest Assessments
- Vendor risk assessments

- Staff training
- Annual Board reporting

Compliance documentation is maintained to demonstrate accountability under Article 5(2) of GDPR.

19. Policy Review

This Policy is reviewed annually or earlier if required by regulatory or organisational changes.