International School of Tallinn

IST DATA PROTECTION POLICY

Introduction

The **International School of Tallinn (IST)** is committed to processing data in accordance with its responsibilities under the relevant national data protection regulations and the **General Data Protection Policy (GDPR).**

The IST obtains, uses, stores and otherwise processes personal data relating to potential staff and students (applicants), current and former staff and students, current and former contractors, website users and contacts, collectively referred to in this policy as **data subjects.** When processing personal data, the IST is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, address, contact information, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

All personal data including racial, political, religious, trade union membership, genetic, biometric, sexual orientation, and health details of individuals from the EU falls under the GDPR's **sensitive personal data** list, that are subjected to a higher level of protection.

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g., on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the IST's behalf must read it.

The Data Protection Officer (DPO) is responsible for ensuring that all IST staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls, and training to ensure that compliance; advising the staff of its obligations under the national data protection legislation and GDPR; manage and keep up to date the **Register of Systems**; and IST's ongoing compliance with this policy. This policy shall be reviewed at least annually.

Regarding any inquiries the Data Protection Officer (DPO) can be reached at office@ist.ee

The Data Protection Policy is a live document and is subject to change whenever the regulations or the sources of provided information change.

Principles

According to the following principles, which are set out in the Article 5 of the GDPR, personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
  Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR) (gdpr-info.eu)

Processing personal data

The purposes to process personal data are to enrol new students and to provide educational service for the students attending the school. The main categories are IST students, their parents/guardians and IST employees/service providers.

IST students and parents/guardians personal data can be processed with reference to:

- visiting the website;
- communication regarding the admission process;
- concluding the schooling contract;
- using the Learning Management System;
- invoicing school fees and providing school lunch;
- the school nurse and SEN department services.

The processed personal data may include: name, ID code, address, phone number, email address, previous and current academic data, financial data, dietary information, health and other above mentioned sensitive data.

The photos of the students can only be used by school when the parent/guardian has signed a written permission.

IST employees and service providers personal data can be processed with reference to:

- visiting the website;
- communication with applicants;
- concluding the employment/service contract,
- employment/service providing.

The processed personal data may include: name, ID code, address, phone number, email address, previous and current academic data, bank account data, language and other skills data, criminal record data, dietary information, health data.

Processing sensitive personal data

IST processes sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation according to the GDPR only if one of the following applies:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or pursuant to contract with a health professional.

Sensitive personal data is processed mainly with reference to school nurse and SEN department services. To find more specific information, click here:
Art. 9 GDPR – Processing of special categories of personal data - General Data Protection Regulation (GDPR) (gdpr-info.eu)

Third-party data processors

Where external persons and/or companies are used to process personal data on behalf of the IST, responsibility for the security and appropriate use of that data remains with the IST. Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken that such security measures are in place;
- a data processing agreement must be signed by both parties.

IST may transfer personal data on legal and contractual bases to:

- the Estonian Education Information System (EHIS);
- the Tallinn Education Department;
- ARNO software system for managing educational services;
- previous and future educational institutions of a student;
- healthcare service providers;
- extracurricular activities service providers;
- IT service providers;
- substitute teaching service providers;
- legal assistance service providers;
- accounting service providers;
- training service providers.

Data subjects' rights

Data subjects have following rights in relation to their personal data is handled by IST:

- to ask for access to their personal data that we hold;
- to withdraw the consent at any time, where the legal basis of our processing is consent;
- to ask us to erase personal data without delay when one of the following applies:
  - the data subject withdraws the consent and there are no legal ground for the processing;
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - for compliance with a legal obligation to which the controller is subject;
- to prevent our use of the personal data for direct marketing purposes;
- to object to our processing of personal data in limited circumstances;
- to ask us to rectify inaccurate data or to complete incomplete data;

- to restrict processing in specific circumstances e.g., where there is a complaint about accuracy, the processing is unlawful;
- to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
- the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the IST;
- to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.

To find more specific information, click here:
Chapter 3 – Rights of the data subject - General Data Protection Regulation (GDPR) (gdpr-info.eu)

Data subject access requests

Data subjects have the right to receive a copy of their personal data which is held by the IST. In addition, an individual is entitled to receive further information about the IST's processing of their personal data as follows:

- the purposes
- the categories of personal data being processed
- recipients/categories of recipient
- retention periods
- information about their rights
- the right to complain to the Data Protection Inspectorate
- details of the relevant safeguards where personal data is transferred outside the EU.

The identity of an individual requesting data under any of the rights listed must be verified. Requests must be complied with, usually within one month of receipt. Any Data Subject Access Request received must immediately be forwarded to the DPO.

Accountability

The IST must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The IST is responsible for, and must be able to demonstrate compliance with, the data protection principles.

The adequate resources and controls must apply to ensure and to document GDPR compliance including:

- appointing a suitably qualified DPO;
- training staff on compliance with Data Protection Law and keeping a record accordingly;
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

IST and DPO responsibilities

IST responsibilities

As the Data Controller, the IST is responsible for establishing policies and procedures in order to comply with GDPR and data protection law.

DPO responsibilities:

- advising the IST staff of its obligations under GDPR and national data protection law;
- monitoring compliance with this policy and other relevant data protection legislation, the IST's policies with respect to this and monitoring training and audit activities relate to GDPR compliance;
- to provide advice where requested on data protection impact assessments;
- to cooperate with and act as the contact point for the Data Protection Inspectorate;
- manage and keep up to date the Register of Systems;
- DPO shall in the performance of her tasks have due regard to the risk associated with processing operations, considering the nature, scope, context, and purposes of processing.

Staff responsibilities

All staff members who process personal data about students, staff, applicants, alumni, or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- all personal data is kept securely;
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- personal data is kept in accordance with the IST's retention schedule;
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO;

- any data protection breaches are swiftly brought to the attention of the DPO and that they support the IST in resolving breaches;
- where there is uncertainty around a data protection matter advice is sought from the DPO.

Where members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection principles.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the DPO.

Limitation of transferring the personal data

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit or send that data to a different country or view/access it in a different country.

The European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms. The countries currently approved can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

To find more specific information, click here: Chapter 5 – Transfers of personal data to third countries or international organisations - General Data Protection Regulation (GDPR) (gdpr-info.eu)

Direct marketing

IST is a subject to certain rules and privacy laws when marketing to our applicants, students, alumni and any other potential user of our services.

For example, a data subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers (e.g. current students/parents) known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services (e.g. a post-graduate course or a professional qualification), and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a data subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. IST is keeping and maintaining accurate **Register of Systems** reflecting the processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

The Register of Systems includes, at a minimum, the name and contact details of the IST as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches are also kept, setting out the facts surrounding the breach, its effects and the remedial action taken.

Security measures

The IST as a controller implements appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.
That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Personal data that is being processed by the ISTI is mainly in a digital form on **Google Suite Environment**. The system can be accessed by using unique usernames and passwords and implements different limitations to authorised access to different groups of employees. It also keeps a log, which allows to determine who and when accessed which data and what changes were made.

The personal data transferred to third-party data processors are protected with contractual means or can be accessed only by using an Estonian ID card.

The personal data which cannot be stored in a digital format (paper documents, transferable data mediums) are kept in locked metal cupboards or in a safe. Only the possessor of the key of the locked cupboard or safe code has the access to delicate personal data.

Email / File Sharing

E-mail Address Naming Policy: firstname.lastname@ist.ee

Upon creation of a new account, a default auto-generated password is assigned to the user's email account, and this is shared directly with the family, staff member, and the office to ensure that the user is able to log in the first time.

- Once logged in, the user is prompted to change their password.
- For primary school students weak passwords are allowed.
- For middle/high school students, teachers, and staff members only strong passwords are allowed.

There are two main organisational security groups, one for all students with limited rights, and no access to the school's shared drives, and one for all staff which enables staff to access the general shared drive for all staff, and only those miscellaneous shares that have been shared with them specifically on top of that.

Learning Management System - Toddle

The Toddle system integrates our Google platform through SSO, meaning that only users who exist in our Google Suite environment can use the platform as a student/teacher, and otherwise they are denied access. Families can create accounts, however they need the unique identifiers for their child(ren) to create and pair their account to their child(ren)'s account(s).

Access to Toddle

Toddle access is based on our internal requirements.

Students: Limited to the student views for their specific class(es) only.
Teachers: Limited to the teacher views for their specific class(es) only.
Curriculum Coordinator: This role gives editor status to the teacher to specific areas within Toddle, however, only those areas assigned to them.
Administrators: full access to the system based on their role within IST.

Security cameras

Security cameras are used to prevent and respond to situations that threaten the safety of students and school staff and to protect school property. A security camera recording may be issued in proceedings for an offence at the request of the authority prosecuting the offence in accordance with the law.
Only employees authorised by the school administration have the right to access the camera recordings. The cameras are installed on the external walls of the school building and indoors, which transmit the image in real time, record it and allow it to be processed and reproduced later. The camera is not allowed to record audio or monitor a specific person, but only a specific area (e.g. corridor, yard area) and what is happening there. The information about the presence of cameras can be seen on the school grounds.
When processing data obtained by cameras, such security measures are used that protect the collected data from unintentional or unauthorised tracking, copying, modification, transfer and deletion. The recording may be transmitted outside the school or given access only if there is a legal basis for doing so (e.g. to the police).

Reporting a personal data breach

The GDPR requires that we report to the Data Protection Inspectorate any personal data breach where there is a risk to the rights and freedoms of the data subject.
Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly.
In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.
IST have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the The Data Protection Inspectorate when it is legally required.
If you know or suspect that a personal data breach has occurred, you should immediately contact the DPO at office@ist.ee and follow the instructions in the personal data breach procedure. You must retain all evidence relating to personal data breaches in particular to enable the IST to maintain a record of such breaches, as required by the GDPR.
DPO shall notify the Data Protection Inspectorate (Andmekaitse Inspektsioon) without undue delay (where feasible, not later than 72 hours after becoming aware of the breach). This obligation does not apply in case the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.