Data Protection Policy

Introduction

The International School of Toulouse (Airbus Mobility SAS) collects and uses personal information about staff, students, parents or guardians and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school/company complies with its statutory obligations.
References to "we", "our", "us" in this policy refer to the International School of Toulouse /Airbus Mobility SAS and its employees when acting in their official capacity.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the EU General Data Protection Regulation (GDPR), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.
All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Definitions

Data Subject	The individual in relation to which the school is holding information about; in our context this is parents, students, staff, sub-contacted employees and suppliers.
Personal Data	Personal information or data is defined as data which relates to a living individual who can be identified from that data.
Sensitive Personal Data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings.

Data Protection Officer (DPO)

Frédéric Fantin fantin_f@intst.net

Principles

In accordance with the requirements outlined in the GDPR:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the GDPR.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Lawful Processing

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained and freely given.
- Processing is necessary for:
    - Compliance with a legal obligation.
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    - For the performance of a contract with the data subject or to take steps to enter into a contract.
    - Protecting the vital interests of a data subject or another person.
    - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Consent

Some data that we collect is subject to active consent by the data subject which is freely given. This consent can be revoked at any time.

Sensitive Personal Data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law. Where legally allowed, when data are being collected, data subjects will be informed explicitly with whom it will be shared. Sensitive data will be shared on a needs basis with appropriate access controls. In the case of surveys, any element where personal opinions may be considered as 'sensitive data' will be treated as such.

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Individuals and data subjects must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required.

Privacy Notice – transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. Privacy notices for staff, parents and students can be found in the annex of this policy as well as on the school website.

Sharing Personal Data

It is necessary to share personal data with third party organisations. It is our responsibility to ensure that the data we share is compliant with the conditions of processing and is shared in a secure manner.

Storing data securely

- In cases when personal data is stored in paper format, it is kept in a secure place where unauthorised personnel cannot access it.
- Secure remote access software is used for accessing school systems from another location.
- All network users have individual logins and network permissions are set correctly so users can only access the data and files they require to carry out their duties
- Devices such as school laptops, tablets and mobile phones should be password protected. Outside school, the utmost care should be taken to ensure devices are locked or turned off when not in use.
- Antivirus and malware software must be kept up to date as well as operating systems on school laptops, tablets and mobile phones.
- Personal data stored on CDs or memory sticks must be locked away securely when not being used.
- Staff and Students must report loss of a school device laptop, tablet etc) immediately to the Principal and the Network Manager.

CCTV

Cameras are installed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. In accordance with the law, the use of CCTV is registered with the CNIL and signs showing the use of CCTV cameras for the purposes of safety and security are displayed at entrances to the site.

CCTV recordings are stored for no longer than 30 days.

Access to CCTV recorded images is strictly controlled by the Principal of the School.

Data Retention and Deletion

We retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but if relevant, the length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines from French/European authorities. Unrequired data will be deleted as soon as practicable.

Data Breaches

Staff should notify the Principal or the DPO if they are concerned about a possible data breach.
If the breach is sufficiently serious to warrant notification to the public, the breach must be reported without undue delay. If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.
All members of staff have an obligation to report actual or potential data protection compliance failures.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts members of the IST community and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Principal or the DPO.

Responsibility:	Principal / Board
Audience:	Public
Updated:	June 2020