King's College
The British School of Latvia

DATA RETENTION POLICY

VERSION 2023

KING'S COLLEGE LATVIA

Data Controller:

King's College, The British School of Latvia (also referred herein as "the School" or "KCL")
Corporate name: King's College Latvia SIA
VAT register: LV40103917732
Address: Turaidas iela 1, Pinki, Babites novads, LV2107 Latvia
Email: dpo@kingsgroup.org

1. INTRODUCTION

This policy is drafted according to the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the Latvian Law on Legal Protection of Personal Data (hereinafter 'Data Protection Law') in force since July 16, 2018, which stipulate that personal data are only collected for specified, explicit and legitimate purposes under principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security) as well as accountability (responsibility), as is wider explained in paragraph C.

According to the principle of STORAGE LIMITATION, organisations are obliged to delete data from their files if no longer needed. In addition, under both regulations, the employees must be compliant with such requirement. In addition, this principle demands strict data retention policies and procedures to track and trace the storage of personal data. This document provides the policy framework through which this effective data management can be achieved and audited.

Apart from monitoring data retention periods, if security requirements are not met and there is a security breach, the fact that excessive data has been retained, and therefore put at risk, is a factor which the Latvian Data State Inspectorate (DSI) can take into account when considering whether to impose a civil penalty and the level of that penalty. According to the European legislation, monetary penalties of up to 4% of annual global turnover or €20 million may be imposed in case of serious contravention of the Data Protection Principles.

2. SCOPE

KCL is acting as a Data Controller and as such, the School must comply with the obligations under the GDPR and the Data Protection Law. The School must be committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the data protection legislation.

All staff working in KCL must have a general understanding of the law and how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All Inspired staff must read, understand and comply with this policy.

KCL staff must not keep personal data for longer than need it. The files and the information stored in them should be periodically reviewed, necessity of such conservation must be documented or proved and consequently erased or anonymised when it is no longer necessary.

3. LIMITATION OF PERIODS

The regulations set out seven key principles that will underpin the correct data processing and consequently, the data retention. These principles are the following: 1*) Lawfulness, fairness and transparency*: personal data shall be collected and processed on legitimate grounds and the schools must provide full transparency and information to the data subjects about how they process their personal data, in order to get an informed decision from them; *2) Purpose limitation:* personal data must be collected for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes; *3) Data minimisation*: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; *4) Accuracy*: accurate and, where necessary, updated. Personal data that is inaccurate or useless for the purposes for which

they are processed, must be erased or rectified without delay; *5) Storage limitation:* personal data must not be kept longer than needed; *6) Integrity and Confidentiality:* personal data must be 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 the appropriate technical and organisational measures. *7) Accountability:* the school shall be responsible and will be able to prove compliance with the previously mentioned principles.

KCL shall consider the principle of STORAGE LIMITATION when collecting and processing a large amount of personal data every year including pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fees and billing collection as well as the many different types of research data used by the School.

In addition, it may be required by law to collect and use certain types of information to follow statutory obligations of public authorities, government and other entities.

Latvian sectorial regulation stipulates different periods and obligations to comply related Social Security, employment records, child protection, business records, tax and finance information, among other companies' documents, in addition to prescription periods that are part of such conservation requirements.

According to the regulations, the school can keep personal data for longer retention periods just for the following reasons:

- Archiving
- scientific or historical research
- statistical purposes
- child protection folders
- legal litigations

The data kept for Archiving, scientific or historical research purposes should be stored always in the school.
KCL must be aware of such regulations and the periods stipulated in order to be compliant with this policy and the schedule describe herein.

4. PERIODICAL REVIEW

Information (whether hard copy or electronic means) will be retained for at least the period specified in the attached retention schedule on a legal basis. When managing records, the School will adhere to the standard retention times listed within that schedule below.

Paper and digital data will be regularly monitored in each department by the Head of each department.

The local Data Protection Officer ("*DPO*"), or KCL Headteacher, supported by the Inspired Global DPO if necessary, will monitor and send a reminder to the school staff at the end of each school year about the data retention requirements and the security measures that must be implemented by each department.

The recommended security measures to store personal data in a safe way may include, among others, locked cabinets, clear desk & screen, passwords and encryption, access control, restricted access to files, business continuity plan, pseudonymisation of personal data, annual review of technical and organisational measures, etc.

The schedule is a relatively long document listing the many types of main records used by the school and the applicable retention periods for each record type in each department. The retention periods are based on business needs and legal requirements; however, these terms must be adapted to the particular needs and usage of every school.

5. DESTRUCTION OF RECORDS

As soon as records have been identified for destruction, they should be disposed in an appropriate way. All information must be reviewed by the Head of Department, before its elimination, to determine if it is expendable and unnecessary, or its destruction should be delayed for any reason, such as potential litigation, complaints or grievances, administrative procedure or audit in progress, among other circumstances. In these cases, the concerned file should be retained.

All paper records containing personal information or sensitive data must be shredded before disposal. It is recommended to hire the appropriate experts on secure and confidential destruction of documents if possible. All electronic information will be deleted securely by the Head of Department and with the IT department support if necessary.

Each department in the school should provide at the beginning of the year the copy of the database of records which have been destroyed to the Local Data Protection Officer. The Head of Department should record in this list at least:

- File reference (or another unique identifier);
- File title/description;
- Number of files; and
- Date of destruction

6. ARCHIVING

Where records have been identified as being worthy of preservation over the longer term, for example the data of students to be transferred in the student file, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives should be maintained. The individual responsible for the archives should have also a database of archived documents according to the practice of the school.

7. RESPONSIBILITY AND MONITORING

The Head of Department has primary and day-to-day responsibility for implementing this Policy among the school staff. The Data Protection Officer, in conjunction with the Head of the school, is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to supply assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them is made aware of and understand this Policy and are given adequate and regular training on it.

8. DATA RETENTION SCHEDULE

This section includes the main retention periods that the Inspired schools must respect, according to the respective specific local legislations and without prejudice to their needs.

The periods are following the order below:

1. *HR DEPARTEMENT*
2. *FINANCE DEPARTEMENT*
3. *ADMISSIONS AND MARKETING*
4. *MARKETING*
5. *TEACHERS*
6. *HEALTH AND SAFTY AND CHID PROTECTION*

1. HR DEPARTMENT

File Description	RETENTION PERIODS
Application forms and interview notes (for unsuccessful candidates)	**6 months** Business interest
HR files successful candidates	**10 years** as of the expiry of the employment contract (AMF/CFT regulations)
Email previous Staff	General employment documentation (i.e. hired employees) is retained for the duration of employment and for **2 to 10 years** thereafter (AMF/CFT regulations)
Payroll	General employment documentation (i.e. hired employees) is retained for the duration of employment and for **2 to 10 years** thereafter (AMF/CFT regulations)

2. FINANCE DEPARTMENT

Budget	**10 years (**AML/CFT regulations and applicable Latvian data retention regime 2015)
Financial statements reports	**10 years** (AMF/CFT regulations)
Profit and loss accounts	**10 years** (AMF/CFT regulations)
Suppliers contract	**10 years** (AMF/CFT regulations)
Taxation and Accounting Records	**5 years** Not less than 5 years as of the end of the financial year (Compliance with the law On Accounting)
Boards Meetings Minutes	**Permanent** Business Interest
Government company decision	**Permanent** Business Interest
Auditor reports	**Permanent** Business Interest

3. ADMISSIONS

Registration form And contract	**10 years** after the end or change of the school (AMF/CFT regulations)
Family details and contacts	**5 years** after the end or change of the school

School Reports	**10 years** after the end or change of the school (AMF/CFT regulations applicable on contractual obligations)
Parental consent forms	**10 years** after the end or change of the school (AMF/CFT regulations applicable on contractual obligations)
Diploma	**10 years** (AMF/CFT regulations applicable on contractual obligations)

All the student's main folder should contain the following information or documents:

- Registration form and signed contract
- Academic information
- Family details and contacts
- Health reports
- School reports
- Diploma
- Parental consent forms
- Familiar status related documents (Court decisions, etc)

4. MARKETING

There are no specific retention periods set under the GDPR, so it is up to your organisation to establish or identify them and any legal limitation law.

The Marketing team should retain the personal data for as long as necessary to fulfil the purpose for which it was collected. Legitimate interest and consent are the legal basis for collecting and processing personal data for marketing purposes. The Personal data used for marketing purposes should be anonymised if it is used for marketing statically raisons.

The mass mailing systems for commercial purposes must have the unsubscribe functionality. The right of withdrawal of consent at any time should be respected and guaranteed.

The photo consent must be written, and they will be valid for one year, but it must be stored in the student file for the maximum time allowed in each country with evidentiary effects in case of conflict.

Maximum retention period for marketing material **is maximum of 2 years.**

5. TEACHERS

The data retained by the teachers should be sorted at the end of the year by each teacher and the not necessary, or essential or not legally required information should be eliminated.

The teacher should transfer the personal data concerning child protection to the child protection officer any data that could be used in civil or penal litigation should be transferred to the child protection officer or to the archives.

All the other personal data of the students should be deleted **5 years after** the end or change of the school of the student.

6. HEALTH AND SAFETY AND CHILD PROTECTION AND LEGAL CLAIMS

Child Protection Documents	**Unlimited** Interest of a Child
Students Health folder	**Unlimited** Interest of a Child
School Plan and Authorisations	**Permanent** Business Interest
Risk Assessments	**Permanent** Business Interest
Visitor form	**1 year** Business Interest
Legal claims or potential legal claims. Proves	**10 years** Limitation period For legal proceeding
All employee medical surveillance records concerning work accident or due to chemical agent, noises exposed in the work	**Unlimited** Business interest
CCTV footage	**2 weeks- blocked 90 days** as of when the recording was made unless a longer retention period is necessary for the purposes of investigating the specific incident