DATA RETENTION POLICY

MAY 2020

UNITED KINGDOM

A. INTRODUCTION

The European Data Protection Regulation 2016/679 (GDPR) does not only apply to companies in the EU but also to companies outside of the EU that market goods or services to EU citizens. It also applies to companies who either control or process data regarding an EU citizen so all schools within Inspired Group must take into account the European regulations in addition to their local legislations.

The GDPR requires 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. Organisations are obliged to delete data from their files if no longer needed. In addition, under the GDPR and local data protection legislation of every country, individuals have the faculty to exercise different rights, but mainly right of access to their personal data. This demands strict data retention policies and procedures to track and trace the personal data. This document provides the policy framework through which this effective data management can be achieved and audited.

If security requirements are not met and there is data loss, the fact that excessive data has been retained, and therefore put at risk, is a factor which the Data Protection Authorities of every country 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 the event of serious contravention of the Data Protection Principles.

Besides the European penalties, all the non-EU laws set forth different sanctions in the event of non-compliance with the aforementioned security measures.

This policy is also drafted under the considerations of the Data Protection Act 2018 ("DPA") and the sectoral laws applicable in data retention.

B. SCOPE

Each Inspired School is a Data Controller and as such, they must comply with the obligations under the GDPR and the local Data Protection Acts and legal bodies. 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 Inspired Schools 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.

Inspired Staff must not keep personal data for longer than they need it.
Each Inspired staff member should be able to justify the reason of storage of each document containing personal data.

Inspired Staff should also periodically review the data that they hold on behalf of their job, and erase or anonymise it when they no longer need it for their job.

Each Inspired Employee must carefully consider any challenges to the retention of data.

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.

Each Inspired School collects and processes a large amount of personal data every year including pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee 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 comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

C. GDPR PRINCIPLES

The GDPR sets 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 demonstrate compliance with the previously mentioned principles.

D. RETENTION SCHEDULE

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 DPO, 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.

E. 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

F. 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.

G. 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 provide assurance that they are effective in creating, maintaining and removing records.

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

H. 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)	**12 months** Recommended practice (CIPD) Defamation Act 1996 1-year limitation (in respect of any shared comments)
HR files successful candidates	**6 years** after the end of employment. The National Archives Retention Scheduling: Employee Personnel Records and CPID Limitation Act 1980
Email previous Staff	**12 months** after the end of employment and archived without deletion until the end of business interest.
Payroll	**7 years** Finance Act 1998 (Schedule 18, paragraph 21)

The Employer must keep prescribed details of any strike, lock-out or protest action involving the employees and should keep records for each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions should be kept permanently.

2. FINANCE DEPARTEMENT

File Description	RETENTION PERIODS
Budget	**7 years** Paragraph 6, Schedule 11, VAT Act 1994 and HMRC Notice 700/21 (October 2013)
Financial statements reports	**7 years** Paragraph 6, Schedule 11, VAT Act 1994 and HMRC Notice 700/21 (October 2013)
Profit and loss accounts	**7 years** Paragraph 6, Schedule 11, VAT Act 1994 and HMRC Notice 700/21 (October 2013)
Suppliers contract	**7 years** After the end of relationship Paragraph 6, Schedule 11, VAT Act 1994 and HMRC Notice 700/21 (October 2013)
Taxation and Accounting Records	**7 years** Paragraph 6, Schedule 11, VAT Act 1994 and HMRC Notice 700/21 (October 2013)
Boards Meetings Minutes	**Permanent** Business Interest
Government company decision	**Permanent** Business Interest
Auditor reports	**Permanent** Business Interest

3. ADMISSIONS AND MARKETING

File Description	RETENTION PERIODS
Registration form And contract	**25 years** from date of birth
Family details and contacts	**25 years** from date of birth
School Reports	**25 years** from date of birth
Parental consent forms	**25 years** from date of birth
Diploma	**25 years** from date of birth

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)

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. The 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 reasons.

The mass mailing systems for sending commercial communications must have the unsubscribing functionality. The right of consent withdrawal at any time and freely must be respected and guaranteed.

*Maximum retention period for consent **is 10 years.***

4. TEACHERS

The data retained by the teachers should be sorted at the end of the year by each teacher and the not needed data 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.*

5. HEALTH AND SAFTY AND CHILD PROTECTION AND LEGAL CLAIMS

File Description	RETENTION PERIODS
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	**12 years** Limitation act
All employee medical surveillance records concerning work accident or due to chemical agent, noises exposed in the work	**Unlimited** Business interest
CCTV footage	**1 month** ICO recommendation