King's Group

DATA RETENTION POLICY

KING'S COLLEGE SCHOOL, PANAMÁ

DOCUMENT VERSION

Version number	Author	Date
V0.1 Creation	Patricia Sarrais (DPO)	May 2020
V0.2 Update	Patricia Sarrais (DPO)	August 2021
V0.2 Approval	Elena Benito Molina (Europe Chief Operations Officer)	August 2021
V0.2 Approval	Nigel Fossey (Headteacher, King's College Panama)	August 2021
V0.3 Update	Patricia Sarrais (DPO)	June 2024
V0.3 Approval	Oliver Proctor (Headteacher, King's College Panama)	June 2024

1. INTRODUCTION

This policy is drafted under the considerations of the Panamanian Data Protection Law No. 81 of March 26th, 2019 as well as the specific laws applicable in data retention.

The Ley 51 de 18 de septiembre de 2009, (also referred as "Law No. 81) requires that personal data are only collected for specified, explicit and legitimate purposes under principles of Loyalty, Purpose, Proportionality, Truthfulness and accuracy, Data security, Transparency, Confidentiality, Legality and Portability.

Companies are obliged to delete data from their files if no longer needed. In addition, under the Law 81, 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.

2. SCOPE

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 and in our case, in King's College Panama, 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 staff must read, understand and comply with this policy.

Data must not be kept for longer than they are needed.

The School's 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 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, government agencies and other bodies.

3. PRINCIPLES OF LAW NO. 81

The school is obligated under the Law No. 81, to abide by the Regulations' principles, which ensure that personal information shall be kept only to preserve:

- Purpose: Personal data must be collected for specific purposes and not subsequently processed for purposes other than those for which they were requested, not kept for longer than necessary for the purposes of the treatment.
- Proportionality: Only adequate, pertinent and limited data is requested in relation to the required purpose.
- Truthfulness and accuracy: They must be exact and respond truthfully to the current situation of the owner of the data.
- Data security: Those responsible for the processing of personal data must adopt measures to guarantee the security of the data and inform the owner, as soon as possible, when the data has been stolen without authorization or there are indications that its security has been violated.
- Confidentiality: All persons involved in the processing of personal data have the obligation to keep secrecy or confidentiality regarding them.

4. DATA 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 data protection officer, 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 of the College must have a record of files with which it works, establishing:

- 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.
It must be created a backup set of records, and it is advisable to store them electronically.

Even if the original records are provided only on paper, they must be scanned and converted to a digital format to be automated. Once the documents are in electronic form, they can be securely stored in a clod storage system, avoiding external backup storage devices, such as an external hard drive, CD or DVD, that can be stolen or lost. These backups must be correctly labelled and identified.

Keeping automated records is the only way to ensure that data are fully protected. With an online backup or cloud storage service, is more possible that documents remain safe.

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 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.

8. CRITERIA OF CONSERVATION

Panamanian sectoral regulations set up periods of conservation for particular records, considering the obligation to comply with legal purposes and the necessity to keep the records in the case there is a legal obligation, exercise of a right or claim that may arise, following the prescription periods. Once such periods have expired, there is not any right or obligation that can be claimed, as due to the passing of time, any action has prescribed.

E.g. Law No. 254 of November 11: Accounting records must be kept and maintained at the latest within four (4) months following the expiration of each fiscal year, (e.g., accounts, tax records, invoicing, etc); Company records: Following Law No. 254, in case of dissolution, the accounting records and supporting documentation or their respective copies for the five (5) years prior to the registration of the dissolution must also be kept by the legal entity and be available for a minimum period of five (5) years from the registration of the dissolution.

After those periods, those documents and the actions that may derive from them, are expired.

9. PENALTIES FOR NON-COMPLIANCE

Article 40 of Law no. 81 determines a a serious infringement in section 6 “store or archive personal data without having the appropriate security conditions provided by this Law or its regulations” which is also referred to the retention of the necessary information during the limited period and under security measures. Its lack of compliance may lead to the closure of the School in addition to personal and corporate criminal and civil responsibilities and high fines that will be assessed by Autoridad Nacional de Transparencia y Acceso a la Información accordingly.

10. 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. HUMAN RESOURCES DEPARTMENT

File Description	RETENTION PERIODS
Application forms and interview notes (for unsuccessful candidates)	**1 year** Article 12 Labor code
HR files successful candidates	**15 years** Article 84-j of the organic law as amended by the Article 47 of Law No. 30 of 1991 Fiscal Code
Email previous Staff	**No time prescribed**
Payroll	**5 years** Article 12 A of the Labor code
Employees general documents	**3 years** Article 12 A of the Labor code

2. FINANCE DEPARTMENT

Budget	**3 years** Article 1652 Código de Comercio
Financial statements reports	**5 years** Article 93 Código de Comercio
Profit and loss accounts	**5 years** Article 93 Código de Comercio
Suppliers contract	**5 years** Article 93 Código de Comercio
Taxation and Accounting Records	**Permanent** Article 264 Código de Comercio
Boards Meetings Minutes	**Permanent** Article 264 Código de Comercio
Government company decision	**Permanent** Article 264 Código de Comercio
Auditor reports	**Permanent** Article 264 Código de Comercio

3. ADMISSIONS AND ADMINISTRATION

Registration form And contract	**25 years** EDUCATION LAW (Decree 305, 2004)
Family details and contacts	**25 years** EDUCATION LAW (Decree 305, 2004)
School Reports	**25 years** EDUCATION LAW (Decree 305, 2004)
Parental consent forms	**25 years** EDUCATION LAW (Decree 305, 2004)
Diploma	**25 years** EDUCATION LAW (Decree 305, 2004)

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 Law No. 81, 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 period of **5 years,** specially related to images (under subject's consent).

5. 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.

6. HEALTH AND SAFETY AND CHILD PROTECTION AND LEGAL CLAIMS

Child Protection Documents	**25 years** EDUCATION LAW (Decree 305, 2004)
Students Health folder	**25 years** EDUCATION LAW (Decree 305, 2004)
School Plan and Authorisations	**25 years** EDUCATION LAW (Decree 305, 2004)
Risk Assessments	**25 years** EDUCATION LAW (Decree 305, 2004)
Visitor form	**25 years** EDUCATION LAW (Decree 305, 2004)
Legal claims or potential legal claims. Proves	**25 years** EDUCATION LAW (Decree 305, 2004)
All employee medical surveillance records concerning work accident or due to chemical agent, noises exposed in the work	**25 years** EDUCATION LAW (Decree 305, 2004)

8. OTHER

CCTV footage	**24** Hours unless a longer period is required by Police and / or Courts or when it is necessary in the course of an investigation
Data Subject requests	During the time necessary to solve the request and until it has been solved and / or closed before the National Authority