Policy

F&B07

TITLE OF POLICY	Data Protection, Management and Retention
COVERAGE	Employees
FIRST RELEASE DATE	31/08/2021
LAST RATIFIED DATE	
DATE FOR NEXT REVIEW	31/08/2022
OWNER	Director of Finance and Business
REVIEWER	Principal

Policy

F&B07

Data Protection, Management and Retention

1. Aim

- To ensure that all information shared in confidence by students and staff will only be used to enhance the safety, well-being and protection of all students and staff members in our care;
- To ensure compliance with the General Data Protection Regulations and relevant legislation connected to this policy;
- To strengthen and unify the safety and security of all data held within the school;
- To ensure the protection of all personal and sensitive data for which we hold responsibility as the Data Controller;
- To ensure the handling of all personal and sensitive data is in line with the data protection principles;
- To allow all school personnel their right to have access to their personal data;
- To allow all parents their right of access to their child's records;
- To ensure vital records are identified and safely stored in the event of a disruption or a crisis affecting the smooth running of the school;
- To ensure compliance with all relevant legislation connected to this policy;
- To have in place an effective records management system;
- To provide a structure on which the everyday running and development of the school is based;
- To provide up to date policies and schemes of work for all curriculum areas;
- To work with other schools and the local authority to share good practice in order to improve this policy;
- To share good practice within the school, with other schools and with the local authority in order to improve this policy.

2. Statement of intent

This policy will be a working document that is fit-for-purpose, represents the school ethos, enables consistency and quality across the school.

We are committed to the protection of all personal and sensitive data for which we hold responsibility as the Data Controller. We believe the handling of such data is in line with the data protection principles and that access to such data does not breach the rights of the individuals to whom it relates.

At all times we ensure that all data is:

- Processed lawfully;
- Obtained and processed for specific and lawful purposes;
- Sufficient, appropriate and not excessive in relation to the precise purpose;
- Accurate and up-to-date;
- Kept for the relevant amount of time;

- Processed in agreement with the individual's legal rights;
- Protected against unlawful processing, accidental loss, destruction or damage;
- Not to be transferred outside Jordan unless the rights and freedom of the individuals are protected.

We believe confidentiality is when someone during a private conversation entrusts another with their secrets and with the confider expecting absolute confidentiality from the confidante. We feel we can only offer limited and not absolute confidentiality at this school as the safety, well-being and protection of our students are the main consideration in all decisions school personnel make.

We stress that school staff must make it clear when in discussion with students or parents/carers that there are limits to confidentiality that can be offered, so that they can make informed decisions about the most appropriate person/s to talk to about the personal matters that have been disclosed.

We are committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected;
- Inform individuals when their information is shared, and why and with whom it was shared;
- Check the quality and the accuracy of the information it holds;
- Ensure that information is not retained for longer than is necessary;
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely;
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Share information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- Ensure our staff are aware of and understand all policies and procedures.

3. Scope

This policy is applicable to:

- All staff, full time and part time, local and expatriates, volunteers and interns who handle and use the school's information whether we hold it on our systems (manual and automated) or if others hold it on their systems for us;
- All parents, whether they are parents of existing, graduating or leaving students;
- All students, whether they are future, existing, graduating or leaving students;

- All Board of Governor members, whether they are current or previous elected members;
- All vendors, third parties, suppliers who are engaged whether directly or indirectly with the school and have access to any data.

4. Unique definitions

4.1 Data

Means information in a form that can be processed. It includes automated data and manual data. Automated data means any information on a computer, or recorded with the intention that it will be processed. Manual data means information that is kept/recorded as part of a relevant filing system. It is the school's responsibility to make sure that this data is protected.

Relevant filing system:

Any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a staff member or students is readily, quickly and easily accessible.

4.2 Data Management

Is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively. The goal of data management is to help Parents, Staff, Board members or any other organisations optimise the use of data within the bounds of the school policy. Data management has a wide scope, covering factors such as how to:

- Create, access, and update data across a diverse data tier;
- Store data across multiple clouds and on premises;
- Provide high availability and disaster recovery;
- Use data in a growing variety of apps, analytics, and algorithms;
- Ensure data privacy and security;
- Archive and destroy data in accordance with retention schedules and compliance requirements.

4.3 Data Retention

Is defining what data should be stored or archived, where that should happen, for what purpose and for what time period.

4.4 Confidential information

This Includes any information which is not publicly known. It can concern technology, business, finance, transaction, personal data related to staff, student, parent or other sensitive data. It includes information which is commercially valuable such as business information, as well as personal information. Examples of confidential information include but are not limited to: any document, discovery, invention, improvement, patent specification, formulations, plans, ideas, books, accounts, data, reports, drafts of documents of all kinds, correspondence, client information, lists and files, decisions, information about employees, strategies, drawings, recommendations, designs, office precedents, policies and procedures, budget and financial information in any form, i.e. physical, electronic, electromagnetic or otherwise.

5. Process and practice

5.1 Student, staff, parent data

Disclosure information will be:

- Passed only to those who are authorised to receive it in the course of their duties, which may in certain circumstances include external agencies;
- Used only for the specific purpose for which it was requested and for which the applicant's full consent has been given;
- Stored separately and securely with access strictly controlled and limited to those who are entitled to see it as part of their duties;
- Destroyed by suitable and secure means and not retained for longer than is necessary.

5.2 SICJ and Board data

Disclosure information will be:

- Passed only to those who are authorised to receive it in the course of their duties, which may in certain circumstances include external agencies;
- Used only for the specific purpose for which it was requested and for which the applicant's full consent has been given;
- Stored separately and securely with access strictly controlled and limited to those who are entitled to see it as part of their duties;
- Destroyed by suitable and secure means and not retained for longer than is necessary.

6. Associated forms and documents

None.

7. Responsibility for the Policy and Procedure

All employees and Governors are expected to have read and understand this policy.

Specific responsibilities include:

7.1 SLT

The SLT will:

- Ensure that all school personnel are aware of and comply with this policy;
- Ensure risk assessments are:
  - ❏ In place and cover all aspects of this policy;
  - ❏ Accurate and suitable;
  - ❏ Reviewed annually;
  - ❏ Easily available for all school personnel.
- Make effective use of relevant research and information to improve this policy;
- Provide guidance, support and training to all staff;
- Monitor the effectiveness of this policy by speaking with school personnel and governors;
- Annually report to the Governing Body on the success and development of this policy

7.2 School Personnel:

School personnel will:

- Annually read and understand this policy;
- Comply with all aspects of this policy;

8. Related information

P&D05 - Professional Code of Conduct
F&B01 - Anti Bribery, Fraud and Corruption
P&D03 - Diversity & Equity
HR14 - Performance Review
HR22 - Whistleblowing