

Data Protection

School Principal:

E-Safety Officer:

Date this policy was reviewed and by whom:

Date of next review and by whom:

Table of Contents

<i>What is this Policy:</i>	3
<i>Scope of the Policy</i>	3
<i>DATA Protection Principal:</i>	3
Obtain and process Personal Data fairly:	3
Consent:	4
Keep it only for specified and explicit lawful purposes:	4
Process it only in ways compatible with the purposes for which it was given initially:	4
Keep personal data safe and secure:	4
Keep personal data accurate, complete and up-to-date:	4
<i>DATA SECURITY</i>	5
<i>At our school we will:</i>	5
<i>Secure Transfer Process:</i>	5
Emails:	5
External Storage devices:	6
Cloud Storage Spaces:	6

What is this Policy:

A Data Protection Policy is a statement that sets out how your organisation protects personal data. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored.

The policy applies to all school staff, parents, students and others, insofar as the measures under the policy relate to them. Data will be stored securely so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data will be protected by the school.

Scope of the Policy

- Personal data is any information that relates to any individual within the school premises, wither that individual is a staff, student, volunteer, a visitor or others.
- The School collects a large amount of personal data every year including: students' records, staff records, names and addresses, examination marks, references, fee collection as well as the many different types of other information.
- In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of governmental Authorities, government agencies and other parties.

DATA Protection Principal:

We will comply with data protection law and principals, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Obtain and process Personal Data fairly:

Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students, etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection legislation and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

Consent:

Where consent is the basis for provision of personal data, (e.g. data required to use the student's photo or any other optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Taryam American Private School will require a clear, affirmative action such as ticking of a box or signing a document to indicate consent. Consent can be withdrawn by data subjects in these situations.

Keep it only for specified and explicit lawful purposes:

The school management will inform individuals of the reasons they collect their data and the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times

Process it only in ways compatible with the purposes for which it was given initially:

Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a 'need to know' basis, and access to it will be strictly controlled.

Keep personal data safe and secure:

Only those with a genuine reason for doing so may gain access to the information. Personal Data is securely stored and protected with computer software and password protection in the case of electronically stored data.

Keep personal data accurate, complete and up-to-date:

Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. Records must not be altered or destroyed without proper authorization.

The school is committed to maintaining these principles and will therefore:

- 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 accuracy of the information it holds
- Ensure the information is not retained for longer than necessary
- 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 subject access requests
- Ensure our staff are aware of and understand our policies and procedures.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

At our school we will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data or their computer is locked when left unattended.
- Transfer data using trusted mediums and devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
 - The data must be encrypted and password protected.
 - The device must be password protected.
 - The device must offer approved virus and malware checking software.
 - The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- All access to the school information management system will be on a need-to-know or least privilege basis.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.

Secure Transfer Process:

We use emails and cloud drives to transfer data, where these are secured methods and are protected from any unauthorized access.

Emails:

We always use the school’s email in all our data transactions either between school members themselves, or while communicating any external party.

External Storage devices:

- The use of removable media is not prohibited within Taryam School ; it is infact an essential part of everyday business.
- The use of removable media to transport non-sensitive data can be done on standard devices.
- Regularly updated Anti Virus software should be present on all machines from which the data is taken from and machines on which the data is to be loaded.
- For sensitive data transferring, make sure to not share the storage device with others, or to make it accessible by any unauthorized person.

Cloud Storage Spaces:

- Make sure to use a trusted cloud service when needed a cloud storage to store files containing information about individuals or other sensitive information.
- Make sure that you have setup the privacy privileges in a way that prevents the entry of any unauthorized persons.

For more details about how to use different types of storage devices and services securely, read the Removeable Media Policy.