SHREWSBURY INTERNATIONAL SCHOOL BANGKOK

Policy Title: Data Protection
Policy Section: Section F - Staffing
Policy Number: F23
Approval:SMT 0335
Publish to:
Policy Compendium
Staff Handbook
Parent Portal
Website

Introduction

In its Mission, The School affirms its commitment to caring for students. In the "Commitment and Renewal" value, The School understands that "it is engaged in a process of continual improvement...and recognises the rapid changes required to keep pace" with the modern world. The Data Protection Policy exists to help The School keep personal data and information private and public information open. This policy is designed for the staff of The School but contains information that is relevant for parents and students and the policy becomes a guidance document for training to all constituencies.

Key Principles

Data held by The School will be:

1. Processed fairly and lawfully;
2. Obtained only for lawful purposes;
3. Adequate, relevant and not excessive;
4. Accurate;

5. Kept up to date and not kept for longer than necessary;
6. Amended regularly to ensure that inaccurate data is not held;
7. Kept secure.

The Data Protection Key Principles apply to data held electronically and in paper files on identifiable individuals including student and staff records.

There are two categories of data acknowledged by The School:

1. Information and Records of staff and, where necessary, dependants - such as:
    - Names, addresses, contacts;
    - Dates of Birth;
    - ID / Passport data;
    - School assessment marks and exam results;
    - Special Educational Needs reports; and
    - Staff Performance Management Reviews.
2. Sensitive Personal Data which will only be recorded where necessary and to which greater levels of security apply such as:
    - Medical and Health;
    - Race;
    - Sexuality;
    - Religion;
    - Criminal Offences;
    - Political opinions;
    - Ethnicity.

These lists are for guidance purposes and are not exclusive.

Processing Data

By "processing data", the school means:

1. Collecting;
2. Using;
3. Disclosing;
4. Retaining; and
5. Disposing.

It is understood that CCTV placement, footage and usage and other technologies (such

as biometric scanning) are also covered by the terms of this policy.

The School processes its data fairly and will ensure that it will

1. have legitimate grounds for collecting and using the personal data;
2. not use the data in ways that have unjustified adverse effects on the individuals concerned;
3. be transparent about how the School intends to use the data, and give individuals appropriate "fair" notice when collecting their personal data;
4. handle people's personal data only in ways they would reasonably expect; and
5. make sure the data is not used for unlawful purposes.

This means that parents, students and staff are provided with "fair notice" in formal school documents (such as Terms and Conditions, Contracts, Policies). They will be told:

1. What is being collected and why;
2. Who is the information going to be shared with.

Physical Security

The School reviews regularly:

1. Its buildings - with the Health and Safety Committee taking the lead role;
2. Its storage systems - with IT Manager taking the lead role;
3. Removable media - with the Human Resources Committee taking the lead role.

The following best practice is undertaken in The School with regular in-service training provided at start of term briefings, INSET, Staff Weekly Briefings and other appropriate training opportunities:

1. Locking of doors in offices with enhanced security measures for areas holding "sensitive information.";
2. Enhanced security measures for areas where sensitive information and data is held (such as HR and visa offices);
3. Locking of filing cabinets within offices (and safe securing of keys);
4. Not leaving printed materials on desks;
5. Not leaving confidential documents unsecured for shredding;
6. Keeping portable electronic devices secure - and locked up when not in use;
7. Keeping an up-to-date log of removable media.

When data and hardware are taken away from school premises (for example on residential trips, educational visits and sports fixtures), the key principles of safe storage continue to apply as the school's data is at its most vulnerable when "off-site".

Electronic Security

Key Principles of electronic security are:

1. Electronic devices themselves (school phones, tablets, laptops etc) must be kept safe and locked away when not in use. The School accepts its responsibility to provide private lockable spaces in classrooms and offices.
2. Information stored electronically should be viewed only by those who need to view it;
3. All staff should choose strong passwords for hardware and software and personal devices / removable hardware (such as usb drives or "thumb drives") should be encrypted.
4. When electronic data is no longer required by the school, it will be deleted properly and permanently.

Using personal devices for school business:

1. All such devices must be kept physically secure, password (or biometrically secured) and encrypted;
2. When colleagues leave the employment of the school or sell / pass on their devices, the school remains responsible for its data and requires colleagues to delete data and access routes to school data. Prior to departure, colleagues are asked to sign a Data Protection checklist to ensure compliance with the security components of the Data Protection policy.

Responsibilities

1. The Board of Governors is responsible for the ownership of this policy and delegates its implementation to The Principal;
2. The Senior Management Team (SMT) is responsible for the drafting, review, monitoring of this policy. This team also has the responsibility for making sure that the staff are well trained in Data Protection and that the policy's Key Principles are well communicated and put into place on a daily basis.
3. Each member of staff has an individual professional responsibility for data protection. He / she must be familiar with this policy and take personal steps to

ensure that its key principles are at the heart of daily professional practice.

4. The Director of ICT and the Director of ICT Support Services have a shared responsibility for raising awareness of Data Protection issues and making sure that advice is given to the SMT regarding policy improvements and amendments.

Subject Access Requests

Individuals have the right to access to information that the school holds about them. Parents have the right in normal circumstances to access information held by the school about their children.

1. If an individual requests information held by the school, the request will:
    - be acknowledged;
    - be logged as a Subject Access Request (SAR) by The Principal;
    - be responded to in writing (including email as an accepted form of communication) within 40 calendar days (including holidays);

There are exceptions to the right of access to information. The school's Terms and Conditions make clear the school's rights in respect of private records:

> *The School shall keep private and confidential records and data of The Student both in digital form stored on computer and in hard copy form stored in personnel files. The School is not obliged to disclose such records and data to parents or students. Any such disclosure is made at the discretion of The Principal. In exceptional circumstances as identified below The School may withhold information from The Parent and The Student even when a Subject Access Request has been made:*
>
> *a. Where The School considers The Student's welfare is at risk and/or*
> *b. considers it is in the best interests of The Student's welfare and/or*
> *c. considers it necessary as part of providing or arranging medical assistance to The Student and/or*
> *d. considers the welfare of other members of The School and/or community to be at risk and/or*
> *e. is required under Thai Law,*
>
> *The Parents authorise The School to disclose information about The Student and/or The Parent to relevant parties on a need to know basis.The School shall manage any disclosure to staff within The School on a need to know basis.*

Sharing Personal Data

The school shares some personal data with outside agencies only where necessary such as:

1. Health authorities;
2. Immigration authorities;
3. Police;
4. Government Departments:
    - Ministry of Education;
    - The Revenue Department;
    - The Labour Department;
    - The Teacher Council of Thailand.
4. Other schools:
    - References;
    - Attendance Data;
    - Police check histories etc.

When data is shared, care is taken to ensure that the transfer is secure and that the information is kept secure and not passed on without approval.

The School Website

The school understands that personal information includes photographs and whenever reasonably possible, staff will be asked for permission for images to be published on the school website.

CCTV

When images are captured of identifiable people, data protection principles apply and Subject Access Requests to The Principal can be made as identified above. The reasons why CCTV is used in the school is made clear in signage at entrances and exits from the school. The locations of CCTV cameras are based upon key principles of Child Protection, Health and Safety and Security and are very carefully considered. CCTV cameras are not sited in private areas and, in normal circumstances, footage is kept for a maximum of one month.

Data Processing

In normal circumstances, the school undertakes its own Data Processing using full time employees working to contractual standards and obligations. From time to time, where data processing is undertaken by third party providers, care is taken to ensure that data is transferred and kept securely. Written agreements (with clear instructions and risk assessments) covering data protection and security are signed - and the school will pursue any breaches of contractual terms in these areas.

Third party providers include:

1. Cloud storage companies;
2. Hard copy storage companies;
3. Shredding companies.

Ownership of Data and the Right to Remove

Within a school environment, the ownership of data requires a common sense approach. For guidance, the following table seeks to clarify ownership issues. This is not an exclusive list but is designed to remind staff of the importance of thinking about the ownership of data. Where a member of staff is uncertain about the ownership of data and the right to remove, clarification should be sought from The Principal:

Data	Ownership		
	School	Individual	Shared
School Policies	x		
Schemes of Work			x
Planning Documentation			x
Lesson Plans			x
Notes (such a guidance notes on a text prepared and studied in school)			x
Performance Management Self Reflection and Analysis		x	

Performance Management Planning Meeting Notes and Observation Feedback			x (restricted as per Performance Management Policy)
Employment Agreements			x
Private medical Records		x	

When a member of staff leaves the employment of the school, a check list of data responsibilities will be provided. Completion of this form and compliance with its terms is a contractual obligation. It covers the following issues:

1. Safe return of all school-owned hardware;
2. Deletion of personal files (including emails) from school networks and hardware with guidance provided by the ICT Support Services Team;
3. Ensuring school owned data is not removed;
4. Ensuring copies of shared-ownership data are properly stored and readily accessible.

Equally, the school will ensure that its data protection obligations are fulfilled in respect of:

1. Deletion of personal information;
2. Temporary storage of historic personal information;
3. Ongoing communications with staff who have left.

Freedom of Information

The school has a publication scheme (Appendix A) which describes the information that is routinely made available and reviewed annually as part of the Data Protection policy. The purpose is to make as much information about the school available with minimum inconvenience and free of charge. The following Classes of Information are presented:

1. Who the school is and what is does
2. Limited Financial Information
3. The school's strategic priorities

4. Decision Making
5. Policies and Procedures
6. Lists and Registers
7. Services Offered

The above Classes of Information will not generally include:

1. Information which is prevented by law from disclosure;
2. Information which is protected from disclosure by the school's terms and conditions and the Data Protection policy;
3. Information in draft / consultation form;
4. Information that is no longer readily available as it is in archive storage.

Wherever possible:

1. the information will be published either on the school's website or, where appropriate, a portal accessed by login and password.
2. the information will be published in English and Thai languages; requests for translated documents will be made on a case-by-case basis by The Principal.

Appendix A - Publication Scheme

1. Who the school is and what it does?
    - The Mission;
    - The School Values.

2. Limited Financial Information
    - Company Accounts;
    - Annual Capital Expenditure;
    - Annual CPD Expenditure.

3. The School's Strategic Priorities
    - School Development Plan;
    - Junior and Senior School Improvement Plans;
    - Departmental Development Plans;
    - Board of Governors: Notes of a Meeting.

4. Decision Making

- Communications Policy (in progress).

5. Policies
    - School Policy Compendium;
    - Staff Handbook.

6. Lists and Registers
    - The School Roll;
    - The Staff Organisation Chart.

7. Services Offered