British School of Ulaanbaatar

5.2 – Data Protection Policy

The British School of Ulaanbaatar collects and uses personal information about staff, students, parents and other individuals in contact with the School. Personal information is defined as data which relates to a living individual who can be identified from that data, or other information held. This information is gathered to enable the School to provide education and other associated functions. In addition, there are certain legal requirements to collect and use information to ensure that the school complies with its statutory obligations to the Ministry of Education in Mongolia.

This policy is intended to ensure that personal information is dealt with correctly and securely. As a British School overseas, our intention is to work to the highest standards locally and internationally, and as such BSU follows the guidance provided by the General Data Protection Regulations and Data Protection Act 2018 from the UK, together with other related legislation. The policy applies to information regardless of the way data is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data must be aware of their duties and responsibilities in adhering to these guidelines.

Data Protection Principles

The Data Protection Act 2018 establishes eight enforceable principles that must be adhered to:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018;
7. Personal data shall be kept secure i.e., protected by an appropriate degree of security;
8. Personal data shall not be transferred to another country or territory unless that country or territory ensures an adequate level of data protection.

The school is committed to maintaining the principles listed above. Therefore, the School commits to the following actions as standard practice.

- Informing individuals why and when information is being collected;
- Informing individuals should information regarding them be shared, including why and with whom it was shared;
- Checking the quality and the accuracy of the information held;
- Ensuring information is not retained for longer than necessary;

- Ensuring that when obsolete information is destroyed, this is done so appropriately and securely;
- Ensuring 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
- Sharing information with others only when it is appropriate to do so
- Ensuring colleagues are aware of and understand our policies and procedures.

Definitions of Personal Data

Personal data includes, but is not limited to:

- School admission and attendance registers
- Students' curricular records
- Annual returns to the relevant authorities
- Reports to parents on the achievements of their children
- Records in connection with students entered for public examinations
- Staff records, including disciplinary and payroll records
- Student disciplinary records
- Records of contractors and suppliers
- Personal information for teaching purposes (assessment data, teacher mark books)

Sensitive data should only be processed if the information has been lawfully and fairly obtained and that the subject has consented. Sensitive data includes:

- Ethnic origin
- Political opinions
- Religious beliefs
- Other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health condition
- Alleged and/or criminal offence
- Proceedings or court sentence

Security Measures and Password Protocols

The School has procedures in place to ensure appropriate use, disclosure and protection of personal data, including sensitive data relating to members of staff and students' records. The school uses physical and electronic safeguards to ensure the security of data.

These include:

- Locks to filing cabinets
- Locks to doors, to offices, filing rooms and computer rooms
- Secure management of the holding and storage of keys
- Installation of antivirus software
- Installation of firewall software/hardware
- Secure data backup procedures
- Separate administration and teaching computer areas

- Good practice relating to passwords, clear screens, locking of computers

It is important that the methods by which individuals access School systems and databases are protected and secure. To do so, all staff must comply with the following requirements:

- Passwords for access to School systems such as ISAMS must be at least eight characters in length.
- Longer passwords and passphrases are strongly encouraged.
- Passwords must be completely unique, and not used for any other system, application, or personal account.
- Passwords must not be shared with anyone (including colleagues or managers) and must not be revealed or sent electronically.
- Default installation passwords must be changed immediately after installation is complete.
- User passwords must be changed every three months. Previously used passwords may not be reused.
- System-level passwords must be changed on a quarterly basis.
- Passwords shall not be written down or physically stored anywhere in the office.
- When configuring password “hints,” do not hint at the format of your password (e.g., “zip + middle name”)
- User IDs and passwords must not be stored in an unencrypted format.
- User IDs and passwords must not be scripted to enable automatic login.
- “Remember Password” feature on websites and applications should not be used.
- All mobile devices that connect to the School networks must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

It is the responsibility of colleagues to ensure compliance with the requirements listed above. Failure to do so, particularly should that behaviour lead to a breach of security and the loss of personal data, would result in disciplinary action.

Sharing of Data and Student consent

Whenever possible, students should be consulted about data sharing and their wishes considered concerning this process. The interests of the child should remain paramount. The exceptions to this are: when there is a legal obligation to share information without the consent and/or knowledge of the student, e.g., situations when the School must act to safeguard a child (see 3.5 – Safeguarding and Child Protection) or when the student is deemed to be unable to make a competent decision concerning the sharing of information about them. In such instances, those who are responsible for the student should be consulted. It should be made clear as early as possible that absolute confidentiality cannot be guaranteed if a student’s own safety or the safety of others is at risk. Where a member of staff believes that there is a risk to the health, safety or welfare of a young person or others, which is so serious as to outweigh the young person’s right to privacy, they should explain this clearly to the student and inform the Headmaster in writing within 24 hours of the conversation with the date and time noted.

Student data will and does need to be shared to facilitate normal School operations. However, the following guidelines should be considered when any personal or sensitive data is shared internally.

Information may be shared

- o for information only (e.g., to ensure others may respond appropriately in the case of classroom management, potential problems)
- o because action is required (e.g., to inform the CPLO in the case of a Child Protection issues)

Information should only be shared

- o on a 'need to know' basis
- o in accordance with legal requirements

Where an individual faces a conflict of interest about whether to disclose information or not

- o the interests of the students take priority
- o other members of staff who share the information should be consulted

When in doubt, information should not be shared unless

- o there is a legal requirement to do so
- o there is a clear benefit to the student to do so
- o that the student will be protected from harm by the disclosure

Potentially, those who work directly with students may need to be informed of confidential information. Sensitive data such as medical information on staff and students should not be displayed in 'public' areas where guests to the school may be admitted. Those responsible for the running and administration of the school may also need to be informed. These include:

- Form Tutors/Class Teachers;
- Teaching Staff;
- Pastoral and Support Staff;
- Parents, Guardians or Carers;
- Heads of School and the HeadMaster;
- Members of the Board of Directors;
- Outside Agencies.

Those responsible for sharing personal or confidential information about students or staff should work together to ensure that such sharing is managed in line with statutory guidance. Responsible staff should meet to discuss and agree on what information should be shared, for what legal or proper purpose, to whom it should be shared and how much information should be disclosed.

Sharing Employee Data

The personal data of employees must not be released to third parties without the individual's consent, unless for specific reasons such as prevention or detection of crime, the health, safety and welfare of other employees or where disclosure is to protect the vital interests of the individual. Ideally, the individual's consent should be obtained in writing. If the school wishes to obtain personal data from a third party, e.g., an employee's medical records, the individual's permission should be requested and obtained.

All requests for disclosure should be submitted in writing on headed paper and given full reasons. Accurate information should be given to potential new employers when the School provides a reference for a current or prior employee.

Rights of Data Subjects

When the School requests personal data they must inform individuals as to why the personal data is being processed and to whom it is being disclosed. Personal data held by the School is reviewed and updated annually as necessary. Personal data is held by the School in accordance with the UK guidelines (see 5.3 – Record Retention Policy). Personal information given in confidence must not be disclosed without consent. Employees should not be the subject of monitoring without good cause.

Individuals have the right to prevent processing, which is damaging or distressing to themselves or others, to prevent processing for direct marketing, ensure that no decision significantly affecting them is based solely on the automatic (electronic) processing of data relating to them e.g., assessing their performance at work. The individual also has the right to rectify, block, erase or destroy inaccurate data on application to the school.

Individuals are not entitled to have access to the following:

- References given by an employer;
- Personal data processed for the purposes of management planning;
- Information about or provided by a third party.

Availability of Data

There is a common misconception that the updating of data is the responsibility of a small number of administrative personnel such as the Registrar, HR or Finance Departments. This cannot be true as these colleagues will not be aware of many changes without those responsible for those areas informing them. The following issues should be noted;

School IT Systems:- The IT team is tasked to address technical hardware problems, ensure that software systems are working correctly on the School IT system (installation and upgrades) and to develop the system as directed by SLT, reflecting the strategy agreed with the Board of Directors. The IT team is not required to enter data or to fix shortfalls in usage of software.

Data Entry:- Where possible, data entry should be undertaken by the individual who knows the information. For example, an individual member of staff should update their personal details on ISAMS, or teachers should update details on students within their own classes. At times agreed and approved by SLT, it is more effective to have one individual inputting data gathered from others to ensure efficiency and accuracy.

Complaints

Complaints regarding the use, disclosure and management of data will be dealt with in accordance with School policy (see 5.13 - Complaints Procedure).

Lead Author: Jonathan Warner	**Date drafted:** April 2020
Date for Review: August 2022	**BoD authorisation:** Confirmed