JEDDAH PREP AND GRAMMAR SCHOOL

Data Protection Policy

Jeddah Prep and Grammar School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. Personal information or data 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 in order to enable it 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 KSA.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with best practice in the UK: that is, following the guidance provided by the UK Data Protection Act 2018 and more recently updated General Data Protection Regulations (GDPR) May 2018, and other related legislation. The policy applies to information regardless of the way it is collected, used, recorded, stored and destroyed, irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Data Protection Principles

The General Data Protection Regulations 2018 has six key enforceable principles that must be adhered to at all times:

- Processed fairly, lawfully and in a transparent manner.
- Used for specified, explicit and legitimate purposes.
- Used in a way that is adequate, relevant and limited.
- Accurate and kept up to date.
- Kept no longer than is necessary.
- Processed in a manner that ensures appropriate security of the data.

Under the GDPR 2018, the legal basis you use to process data should be included in your record of processing.

T**he six legal bases:**

- **Consent**: the individual has given consent for you to process their personal data for a specific purpose
- **Contract**: the processing is necessary for a contract you have with the individual
- **Legal obligation**: the processing is necessary for legal reasons
- **Vital interests**: the processing is necessary to protect someone's life
- **Public task:** the processing is necessary for you to perform a task in the public interest
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data that overrides those legitimate interests.

General Statement

The school is 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 our policies and procedures

Security Measures in Place

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 pupils' 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 anti-virus software
- Installation of firewall software/hardware
- Secure data backup procedures
- Good practice relating to passwords, clear screens, locking of computers
- Separate administration and teaching computer areas

Personal Data Covered by the Act

This includes, but is not limited to:

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

Sensitive Data

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
- Biometric information
- 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

Sharing of Data and Pupil consent

The interests of the pupil should remain paramount at all times. Whenever possible, pupils should be consulted and their wishes taken into account concerning the sharing of information about them. The exceptions to this are: when there is a legal obligation

to share information without the consent and/or knowledge of the pupil, e.g., child protection; or when the pupil is deemed to be unable to make a competent decision (based on level of maturity) concerning the sharing of information about them.

In such instances, those who are responsible for the pupil should be consulted. It should be made clear as early as possible that absolute confidentiality cannot be guaranteed if a pupil'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 clearly explain this to the pupil and inform the Headmaster.

Sharing data within the school

Those responsible for sharing personal or confidential information about pupils or staff should work together to ensure that such sharing is handled 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 reasonably disclosed. Sensitive data such as medical information on staff and pupils should not be displayed in 'public' areas where guests to the school may be admitted.

Who needs to know?

Potentially, those who work directly with pupils may need to be informed of confidential information. Those responsible for the running and administration of the school may also need to be informed. These include:

- Form Tutors and Class Teachers,
- Teaching Staff,
- Pastoral and Support Staff,
- Parents,
- Guardians or Carers,
- Heads of School
- Headmaster
- Chair of Governors
- Outside Agencies e.g. the Police

Basis for sharing information

Information may be shared

- for information only (e.g. to ensure others may respond appropriately in the case of classroom management, potential problems)

- because action is required (e.g. to inform the CPLO in the case of possible Child Protection issues)

Information should only be shared

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

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

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

When in doubt, information should not be shared unless

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

Disclosure of Data - Staff

Personal data cannot 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 when supplying a reference for an employee or ex-employee.

Rights of Individuals

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 for **seven years**. 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.

Exemptions

Individuals are not entitled to have access to the following:

- References given by an employer
- Personal data processed for the purposes of management planning e.g. pay reviews, promotion etc.
- Information about or provided by a third party

Availability of Data

There is a common misconception that the updating of data, particularly electronic data, is the responsibility of a small number of administrative personnel such as the IT team, Accounts Department, HR or Reception. This cannot be true as they will not be aware of many changes without those responsible for those areas informing them of changes. In addition, passing this information to a central point is no longer efficient, given the ease with which individuals can update data, as it delays updating, is open to misinterpretation of the information to be entered and overloads key critical points. Therefore in principle:

- **School IT System:** The Head of IT is responsible for ensuring that the IT system, both hardware and software, is available for all users. The IT team is there 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 Governors. The IT team is not there to enter data or to fix shortfalls in use 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 SIMS or teachers should update details on pupils within their own classes. However, in certain cases, it is more effective to have one individual inputting data gathered from others to ensure time efficiencies or to control data changes.
- **Process/Programme Issues.** Certain systems, such as SIMS, Firefly and SOLUS can be upgraded to meet better the Schools' needs.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the Headmaster, or nominated representative.

Date of Issue: 30th November 2020	**Reviewer:** Headmaster, SLT
Date for Review: 30th November 2022	**Approved:** Board of Governors