DATA PROTECTION POLICY

GLOSSARY OF KEY TERMS

"**Data Controller**" is the person or organisation which determines the purposes and means of the processing of personal data. For the purpose of this policy the School itself is the Data Controller.

"**Data Subjects**" means any living individuals whose data the Data Controller processes.

"Individuals" means, for the purpose of this policy, an adult who is a member of staff, or a volunteer or someone who has parental responsibility for a pupil or prospective pupil at the School.

"**Processing**" means any action in relation to that personal data, including filing and communication.

"**Personal Data**" includes everything from which a Data Subject can be identified. It ranges from simple contact details via personnel or pupil files to safeguarding information, and encompasses opinions, file notes or minutes, a record of anyone's intentions towards that person, and communications (such as emails) with or about them.

"Sensitive Personal Data". Some categories of Personal Data are designated "**Special Category Data**" under the GDPR. These comprise data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health or data concerning a natural person's sex life or sexual orientation; and biometric data. Extra safeguards are provided by law for processing of such data.

"Privacy and Compliance Officer". The School has appointed the Bursar as Privacy and Compliance Officer who will deal with all requests and enquiries concerning the School's uses of personal data and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

INTRODUCTION

Everyone has rights with regard to the way in which their personal data is handled. During the course of the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

This Policy covers the School's acquisition, handling and disposal of the personal and sensitive personal data it holds on all Staff, including temporary staff, agency workers, volunteers, parents and pupils. It also applies to Governors and contractors. It explains the School's general approach to data protection which is to ensure that individual's personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that the School complies with the Data Protection Act 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR) which become law on 25th May 2018.

THE PRINCIPLES

The following six principles relate to the processing of Personal Data:
Personal Data must be

- Processed fairly, lawfully and in a transparent matter
- Used for specified, explicit and legitimate purposes
- Used in a way that is adequate, relevant and limited
- Accurate and kept up to date
- Not kept for longer than is necessary
- Processed in a manner that ensures appropriate security of the data

PROCESSING OF PERSONAL DATA
The School shall only process personal data for specific and legitimate purposes. These are:

- providing an education, training and pastoral care.
- providing activities for pupils and parents - this includes school trips and activity clubs.
- providing academic, examination and references for pupils and staff.
- protecting and promoting the interests and objectives of the School - this includes fundraising.
- safeguarding and promoting the welfare of pupils.
- monitoring pupils' and staff's email communications, internet and telephone use to ensure pupils and staff are following the School's IT Acceptable Use Policy.
- promoting the School to prospective pupils and their parents.
- communicating with former students.
- for personnel, administrative and management purposes.
- fulfilling the School's contractual and other legal obligations.
- providing pupils and staff with a safe and secure environment including images on CCTV – all cameras around the School carry appropriate warning signs as to their operation. They are used for the purpose of detecting crime, ensuring personal security and the welfare of staff and students and the protection of the working environment. Images are kept no longer than 14 days to meet these objectives, however, in certain circumstances such as an on-going investigation into criminal activity certain relevant images may be kept for longer but no longer than necessary to complete any such investigation.

If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the consent of the data subject.

The School shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

The School shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission. This applies even if the transfer is to a student's parents or guardians living outside the EEA**.**

The School shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the School's Records Management Policy. Records containing personal data should not be deleted without authorisation from the Privacy and Compliance Officer.

The School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

Sensitive Personal Data
The School has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

- Explicit consent of the data subject must be obtained
- Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
- Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
- Data manifestly made public by the data subject
- Various public interest situations as outlined in the General Data Protection Regulations 2018

INFORMATION AND EXPLANATION

Being transparent and providing accessible information to individuals about how the School will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a Privacy Notice.

The purpose of the Privacy Notice is to ensure that the School's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

A copy of the School's Privacy Notice can be found on the School's website.

PROTECTING CONFIDENTIALITY

Disclosing personal data within the School. Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the data subject, unless they need to know it for a legitimate purpose.

Disclosing personal data outside of the School. Sharing personal data with others is often permissible so long as doing so is fair and lawful under the GDPR. However, staff should always speak to the Privacy and Compliance Officer if in doubt, or if staff are being asked to share personal data in a new way.

Before sharing personal data outside the School, particularly in response to telephone requests for personal data, staff should:

- make sure they are allowed to share it – that they have the necessary consent;

- ensure adequate security. What is adequate will depend on the nature of the data. For example, if the School is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; paper information should be sent by courier or recorded delivery, First or Second Class post is not considered secure enough and

- make sure that the sharing is covered in the privacy notice.

The School should be careful when using photographs, videos or other media. Specific guidance on this is provided in the School's policy on 'Taking, Storing and Using Images of Pupils'.

INFORMATION SECURITY

Information security is the most important aspect of data protection compliance. The School shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the School shall take appropriate steps to prevent these events happening. In particular:

- paper records which include personal data shall be kept in a cabinet or office which is kept locked when unattended.

- the School uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.

- staff must not remove personal data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the IT Technician.

- staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

RIGHTS OF INDIVIDUALS

Individuals are entitled to know whether the School is holding any personal data which relates to them, what that information is, the source of the information, how the School uses it and to whom it has been disclosed. This is known as a Subject Access Request.

Any member of staff wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Privacy and Compliance Officer.

Any member of staff who receives a request for information covered by this policy must inform the Privacy and Compliance Officer as soon as is reasonably possible, normally on the same day. This is important as there is a statutory procedure and timetable which the School must follow. The School has only one month to respond to a Subject Access Request from whenever the request is received.

Individuals have a right to ask the School not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

Individuals have a right to ask for incorrect personal data to be corrected or annotated.

Individuals have the right to object to any of their personal data being processed and to have this data erased.

Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.

Individuals have the right to request their personal data is transferred to another data controller in a commonly used format.

Individuals have the right to complain about the processing of their personal data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.