Data Protection Policy

The Proprietor of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions. The Head of Business/Head of Education and the Proprietor of this School intend to comply fully with the requirements and principles of the Data Protection Act 1985, Data Protection Act 2003 and the General Data Protection Regulations (GDPR). All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the school's Data Protection Policy is available from the school office. General information about the GDPR can be obtained from the Information Commissioner's Office (www.ico.org.uk).

Fair obtaining and processing

The School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

- Processing means obtaining, recording or holding the information or data or carrying out any set operations on the information or data.
- Data subject means an individual who is the subject of personal data or the person to whom the information relates.
- Personal data means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
- Parent includes any person having parental responsibility or care of a child.

Registered purposes

The Data Protection Registration entries for the School are available for inspection, by appointment, at the school office. The Head of Education or the Data Manager, are the persons nominated to deal with Data Protection issues in the School. Registered purposes covering the data held at the school are listed on the School's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data integrity

The School undertakes to ensure data integrity by the following methods:

Data accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments. Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, the school will try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Proprietor for his judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data adequacy and relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The requirement for schools to provide regular Pupil Census and Work Force Census reports ensures a regular check of all data held. The school Data Manager will amend any data that is incorrect.

Length of time

The school does not maintain or store information unnecessarily.

The length of time that the school holds any particular data can be found in the school's Retention Guidelines document.

Subject access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the School's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing subject access requests

Requests for access must be made in writing to the Head of Education or the Head of Business. Pupils, parents or staff may submit a request in writing to the School and the School will respond in not more than 30 days from the request

date. The School will first satisfy itself that the person is correctly identified and that they have an entitlement to the information.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

Authorised disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

The guidelines under which this can happen are as follows:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Use of pupil photo and course work by the school in school publications and on the school website unless there is a formal objection in writing prior to the pupil joining the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Officers and IT personnel working on behalf of the school are contractually bound not to disclose personal data.
- Professionals and third parties working with or on behalf of the school on a strictly need to know basis in order to do their work.
- Disclosures of information to other schools regarding fee payment records, whether or not the information being communicated is also held in machine- readable form.
- At the request of law enforcement agencies.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

Data and computer security

The School has deployed a Management System which holds all confidential data pertaining to pupils and some data relating to staff. The data within the system is protected by password and user level access.

The School undertakes to ensure security of personal data by various approved methods, including limiting access rights, password controls and a firewall.

School laptops, computers and storage media are not allowed to leave the school premises without approval on each occasion.

Requests for data to leave the school premises, for example hardcopy for a school trip, are collected from reception and are returned to reception promptly after the trip.

Physical security

Appropriate building security measures are in place, such as alarms, CCTV and deadlocks. Only authorised persons are allowed in the server room. Disks and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Procedural security

In order to be given authorised access to the shared computer network, staff will first have undergone an enhanced police check and will also be made aware of the school's required Code of Conduct through induction training. Induction training will ensure staff have knowledge of school protocols and procedures around data protection and will fully understand the need for confidentiality.

Overall security policy for data is determined by the Proprietor and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. Any queries or concerns about security of data in the school should in the first instance be referred to the Head of Data & Attainment.

Individual members of staff can be personally liable in law under the terms of the GDPR. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

This Policy is reviewed every 3 years in line with guidelines from the DfE.

Data Protection Act 1998 – Sensitive Personal Data:

Data which relate to a living individual who can be identified:

(a) From those data; or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller;

GDPR Sensitive Personal Data:

(a) The ethnic or racial origin of the data subject

(b) Political opinions

(c) Religious beliefs or other beliefs of a similar nature

(d) Whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation Act 1992)

(e) Their physical or mental health and condition

(f) Their sexual life

(g) The commission or alleged commission by him of any offence

(h) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.