DATA PROTECTION POLICY

Objective
To provide our students with a first class education we collect and use the personal information of staff, pupils, parents and other individuals, who are referred to within this policy as 'data subjects'. The aim of this policy is to protect the fundamental rights and freedoms of these data subjects

Procedure
The Data Protection Act 2018 controls how personal information is used by organisations, and is the UK's implementation of the General Data Protection Regulation (GDPR). All staff involved with the collection, processing and disclosure of personal information are individually responsible for adhering to data protection legislation, together with the procedures outlined in this policy.

'**Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

Data protection principles
All staff using personal data must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, up-to-date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Special categories of personal data
There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

Date reviewed: September 2023 (DAN)
Review date: September 2024

Data subject rights
Under the Data Protection Act 2018, data subjects have the right to find out what information organisations store, collect and process about them. This includes the right to:

- be informed about how their data is being used
- access their personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of their data
- data portability (allowing you to get and reuse your data for different services)
- object to how their data is processed in certain circumstances.

Data Protection Officer (DPO)
The role of DPO is defined by law, and GDPR states that; '*Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.*'

GDPR provides guidance on the role of a DPO. It advises that the data protection officer has to:

1. inform and advise the data controller and the employees who carry out processing of their obligations
2. monitor compliance with the Regulation, including assigning of responsibilities, raising awareness and staff training
3. provide advice where requested as regards the data protection impact assessment
4. cooperate and act as the contact point for the Information Commissioner's Office (ICO)

Independent Regulatory Body
The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Privacy notice
The GDST's privacy notice provides a summary of how and why we process personal information.

Procedures
The following sections provide further information on how the data protection principles should be applied.

Information access (also referred to as Subject Access Request - SAR)
Data subjects have rights to access to personal information held or processed by the GDST.

Data breach
A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Minimisation
Data processed must be limited to what is necessary for the purpose for which it is processed. Staff should consult with the DPO before creating User Defined Fields in any application that will collect special categories of personal data

Retention of personal information

Data must not be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Legal basis for processing personal information

We use a number of different legal bases for processing personal information.
Where no other legal basis exists for processing an individual's personal data we will seek their consent. Any request for consent must be presented in a way that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

An individual has the right to withdraw his or her consent at any time, and it must be as easy to withdraw consent as to give it in the first place.

Children and data protection

Children must be afforded particular protection when their personal information is being processed as they may be less aware of the risks involved.

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing; and have their personal data erased.

Where we rely on consent to process a child's personal data we must ensure the child understands what they are consenting to. When seeking consent we must recognise that there may be a perceived imbalance of power between the person requesting the consent and the child and we must ensure any imbalance is not exploited, even if this is unintended. To ensure students' rights are protected, ordinarily;

- In our Junior and Prep schools we will seek a parents' consent to process a student's personal data.
- In our Senior Schools we will seek both the student and parents' consent to process a student's personal data, and may not treat this as true consent unless both agree.
- In our Sixth Forms, we will seek our students' consent to process their personal data.

The ICO provides further information on protecting the rights of children. Further advice may be sought from the legal department or Data Protection Officer at Trust Office.

Security of personal information.

Our information security policy deals with the confidentiality, integrity and availability of personal information.

Clear desks

All staff are required to ensure that all confidential or restricted information in hardcopy or electronic form is kept secure, in particular;

- Computer workstations must be 'locked' when a workspace is unsupervised.
- Any Confidential or Restric
- ted information must be removed from desks and locked in a drawer or filing cabinet when the desk is unoccupied and at the end of the work day.
- Filing cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not supervised.

Contracts with data processors

Whenever an arrangement is entered into with a data processor who will have responsibility for holding and/or processing GDST data, including personal data, a formal contract containing appropriate safeguards must be drawn up with that data processor that meets the standards outlined in Article 28 of GDPR

Retention of personal information by staff on GDST systems.
All staff are provided with a GDST Google and Microsoft Office 365 account, together with a GDST email account for use with, and storage of, information relating to GDST business.

Staff should not transfer digital content containing the personal information of students or parents, or work-related content containing the personal information of staff out of the GDST network, GDST approved third party applications, Google or Office 365 environment.

A 'digital first' culture is promoted within the GDST, and staff should not print paper records unless this is necessary.

The GDST retains the intellectual property rights (IP) of all material produced by GDST employees' during the course of their employment, and this material may not be retained or used for other purposes by individuals beyond their period of employment without the written permission of a line manager.

Special Categories of Personal Information

The following activities involve the processing of special categories of personal information and additional guidance is provided to support this.

1. Medical records
2. Safeguarding and Pastoral
3. Special educational needs and disability (SEND)
4. School trips