Data Protection Policy

1. Introduction

The College must comply with the European Union General Data Protection Regulation (GDPR), UK Data Protection Act 2018 and other relevant legislation protecting privacy rights.

Spurgeon's College is registered with the Data Protection Commissioner.

The College needs to hold and to process large amounts of personal data about its students, employees, applicants, alumni, contractors and other individuals in order to carry out its business and organisational functions.

Data Protection law defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 natural person. This information is often referred to as person identifying information (PII) by the College and for the purposes of this Policy should be considered to have the same meaning as personal data as defined by the legislation.

2. Purpose

Compliance with legislation will be achieved through the implementation of controls and responsibilities including measures to ensure that:

- Personal data is processed lawfully, fairly and transparently. This includes the provision of appropriate information to individuals upon collection of their data by the College in the form of privacy or data collection notices. The College must also have a legal basis to process personal data;

- Personal data is processed only for the purposes for which it was collected;

- Personal data is accurate and where necessary kept up to date;

- Personal data is adequate, relevant and not excessive for the purposes for which it was collected;

- Personal data is not kept for longer than necessary;

- Personal data is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that personal data, both manual and digital, are subject to an appropriate level of security when stored, used and communicated by the College, in order to protect against unlawful or malicious processing and accidental loss, destruction or damage. It also includes measures to ensure that personal data transferred to or otherwise shared with third-parties have appropriate contractual provision applied;

- Personal data is processed in accordance with the rights of individuals, where applicable. These rights are:

- The right to be informed;
- The right of access to the information held about them by the College (through a subject access request);
- The right to rectification;
- The right to restrict processing;
- The right to erase;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling;

- The design and implementation of College systems and processes must make provision for the security and privacy of personal data, including a Data Protection Impact Assessment;

- Personal data will not be transferred outside of the European Economic Area (EEA) without the appropriate safeguards in place;

- Additional conditions and safeguards must be applied to ensure that more sensitive personal data (defined as Special Category data in the legislation), is handled appropriately by the College. Special category personal data is personal data relating to an individual's:

- Race or ethnic origin;
- Political opinions;

- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data (where used for identification purposes);
- Health; or
- Sex life or sexual orientation.

In addition, similar extra conditions and safeguards also apply to the processing of the personal data relating to criminal convictions and offences.

3. Scope

This Policy applies to:

- All personal data held and processed by the College. This includes expressions of opinion about the individual and of the intentions of the College in respect of that individual. It includes data held in any system or format, whether electronic or manual;

- All members of staff, as well as individuals conducting work at or for the College and/or its subsidiaries, who have access to College information (”staff”). This includes temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the College and suppliers(this list is not intended to be exhaustive); and

- All locations from which personal data is accessed including off-campus.

4. Responsibilities

4.1 College Responsibility

As the Data Controller, the College is responsible for establishing policies and procedures in order to comply with data protection law.

4.2 Data Protection Officer responsibilities

The Data Protection Officer (DPO) is responsible for:

- Advising the College and its staff of its obligations under GDPR;

- Monitoring compliance with this Regulation and other relevant data protection law, the College’s policies with respect to this and monitoring training and audit activities relate to GDPR compliance;

- To provide advice where requested on data protection impact assessments;

- To cooperate with and act as the contact point for the Information Commissioner's Office;

- The DPO shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

4.3 Staff Responsibilities

Staff members who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- All personal data is kept securely;

- No personal data is disclosed either verbally or in writing, accidentally or otherwise to any unauthorised third party;

- Personal data is kept in accordance with the College's retention schedule;

- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer;

- Any data protection breaches or near misses, are swiftly brought to the attention of the DPO and that they support the DPO in resolving breaches;

- Where there is uncertainty around a data protection matter advice is sought from the DPO;

Where members of staff are responsible for supervising students doing work which involves the processing of personal information for example in research projects) they must ensure that those students are aware of the Data Protection principles.

All employees must complete the relevant training provided to support compliance with this policy.

4.4 Third-Party Data Processors

Where external companies are used to process personal data on behalf of the College, responsibility for the security and appropriate use of the data remains with the College.

Where a third-party data processor is used:

- A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;

- Reasonable steps must be taken that such security measures are in place;

- A written contract establishing what personal data will be processed and for what purpose must be set out;

- A data processing agreement, available from the DPO, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the DPO.

4.5 Contractors, Short-Term and Voluntary Staff

The College is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition managers should ensure that:

- Any personal data collected or processed in the course of work undertaken for the College is kept securely and confidentially;

- All personal data is returned to the College on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and the College receives notification in this regard from the contractor or short term/voluntary member of staff;

- The college receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;

- Any personal data made available by the College, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the College;

- All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

4.6 Student Responsibility

Students are responsible for:

- Familiarising themselves with the Privacy Notice provided when they register with the College;

- Ensuring that their personal data provided to the College is accurate and up to data.

5. Data Subject Access Requests

Data subjects have the right to receive a copy of their personal data which is held by the College. In addition, an individual is entitled to receive further information about the College's processing of their personal data as follow:

- The purpose;
- The categories of personal data being processed;
- Recipients/categories of recipient;
- Retention periods;
- Information about their rights;
- The right to complain to the DPO;
- Details of the relevant safeguards where personal data is transferred outside the EEA;
- Any third-party source of the personal data.

Personal data should not be disclosed to third parties without proper authorisation.

6. Record Keeping

The College keeps full and accurate records of all our data processing activities, including records of data subjects' Consents.

Records of personal data breaches must also be kept, setting out:

- The facts surrounding the breach;
- Its effects; and
- The remedial action taken.

7. Monitoring Compliance

This policy is subject to internal monitoring and auditing throughout the College, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement.

Compliance with the act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may be treated as misconduct under the Colleges disciplinary policy and could lead to disciplinary action.

Document control box			
Title	Data Protection Policy		
Date approved	July 2018	Implementation date	July 2018
Next review date	July 2020		
Version	2	Supersedes version	1
Approving body		Governors	
Quality Code consulted			
Member of staff responsible		Director of Operations	