St Gabriel's
Your Route to Success

Including Sandleford, our Early Years Foundation Stage provision

Data Protection Policy

Authorised by	resolution of the Board of Governors
Date	Spring 2018 – (Version 1-0-0)
Reviewed	

Purpose
This policy details the approach taken by St Gabriel's to Data Protection. It explains how we process data in a lawful, fair, transparent and secure way in accordance with the General Data Protection Regulations 2018 (GDPR). The school is registered with the Information Commissioner's Office as a Data Controller (registration number Z548555X.)

The policy should be read in conjunction with
- Privacy Notices for prospective parents and pupils, parents and pupils, workers and alumnae;
- ICT Acceptable Use Policies for workers and pupils;
- Bring Your Own Device Policies;
- Remote Working Policy;
- Taking, Storing and Using Images of Children Policy;
- CCTV Policy;
- Retention of Records Policy;
- Subject Access Request Procedure;
- Data Breach Procedure.

The school will take all reasonable steps to ensure compliance with all the requirements of the GDPR.

Scope and Defintions
This policy applies to all members of the school community including workers, pupils and visitors. The GDPR regulates all of a Data Controller's use of Personal Data, including Sensitive or Special Category Personal Data. It applies to the collection, processing, sharing, storage and deletion of this data. It applies to both electronic and paper data.

A *Data Controller* is defined as an individual or organisation that determines the purposes and means of processing personal data. It may have *Data Processors* working on its behalf who are responsible for processing personal data for the school who retains overall responsibility for the processing and security of this data.

Personal Data is defined as information that covers both facts and opinions about an individual where that data identifies an individual. This individual is known as the *data subject*. For example, it includes information about a member of staff such as name and address and details for payment of salary or a pupil's attendance record and academic results. *Sensitive or Special Category* data is personal data that includes some or all of that individual's race, ethnic origin, political affiliation, religion, details of any trade union membership, genetic information or biometrics (where used for ID purposes), health, sex life or sexual orientation.

Roles and Responsibilities
The school shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the General Data Protection Regulations to ensure all data is:-
- Fairly and lawfully processed;
- Processed for a lawful purpose;
- Adequate, relevant and not excessive;

- Accurate and up to date;
- Not kept for longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

The school is committed to maintaining a transparent and accountable approach to Data Protection at all times and will therefore:

- Inform individuals why the information is being collected when it is collected;
- Inform individuals when their information is shared, including why and with whom it was shared;
- Share information with others only when it is legally appropriate to do so or our policies and privacy notices allow us to do so;
- 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;
- 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, including those around responding to Data Breaches;
- Follow procedures to risk assess any new use of personal data within the school (see below).

All members of the school community should be familiar with and follow the directions contained in the policies and procedures listed at the beginning of this policy.

Data Protection Impact Assessments.

A Data Protection Impact Assessment must be carried out when any new processing of data could result in a high risk to the rights of an individual. This assessment should:

- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

The school should consider whether the new use of existing data, or the collection of additional data will involve:

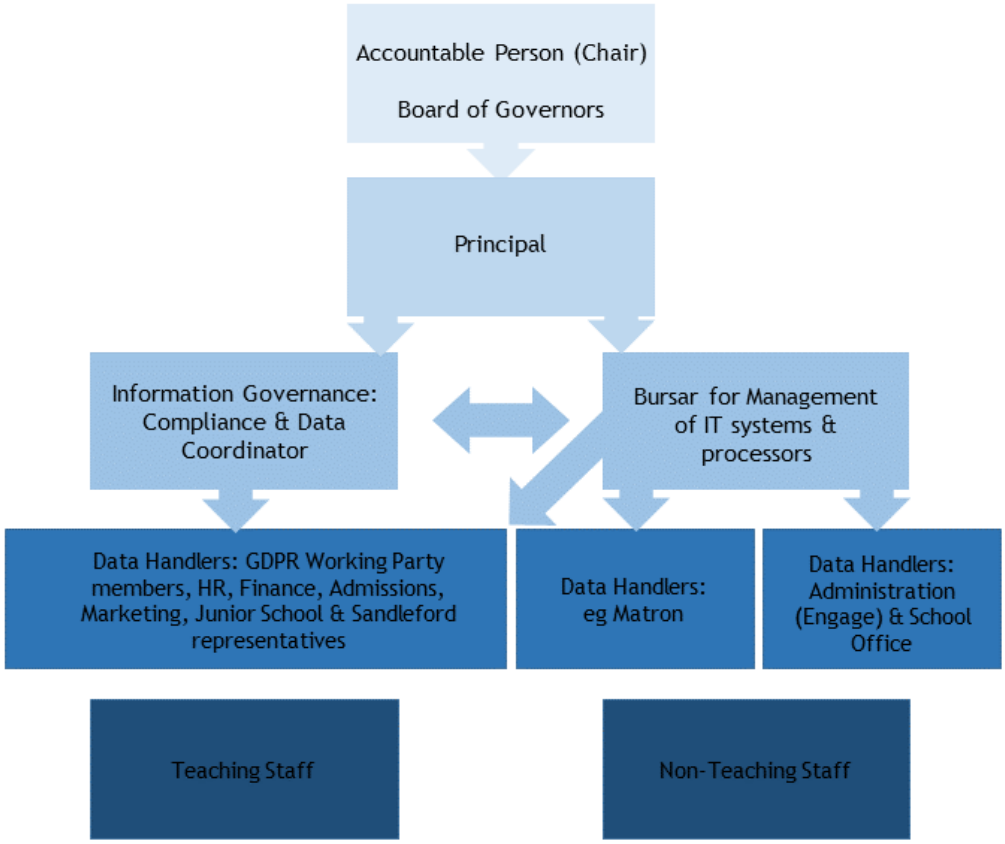
- Processing special category data or criminal offence data on a large scale.
- Using new technologies;
- Processing biometric or genetic data;
- Processing personal data in a way which involves tracking individuals' online or offline location or behaviour;
- Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- Processing of sensitive data or data of a highly personal nature not already used by the school.

Any data handler considering new processing or collecting new data should contact the Data Protection Coordinator or the Bursar.

Information Governance

Responsibility for Information Governance rests with the most senior level of accountability, specifically the Board of Governors, however, support is provided through a robust framework for managing Information Governance that extends throughout the School and reflects the various responsibilities of Information Governance.

The chart below reflects the current information governance structure.



Date	Change History
April 2018	Policy written