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	Spring 2020 (Version 1-0-1)

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) and the Data Protection Act 2018. 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 Policy;
- 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 Definitions
This policy applies to all members of the school community including workers, pupils and visitors. The GDPR regulates all 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 a living 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.

A *Personal Data Breach* occurs when a personal data is accidentally or unlawfully destroyed, lost, altered, or where there is unauthorised access to or disclosure of personal data. The School has a separate Data Breach Procedure which details the actions to be taken in this situation.

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this or any other of the data protection policies may result in disciplinary action.

Where the School shares personal data with third party data controllers (which could include other schools, parents, or appropriate authorities) each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality.

Any contractor acting as a data controller in their own right, will be expected to do so lawfully and to the standards and best practice of the school.

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 in a transparent manner, ensuring that there are lawful grounds for data processing;
- Collected for specific and explicit purposes and only for the purpose it was collected;
- Relevant and limited to what is necessary for the purposes it is processed;
- Accurate and kept up to date;
- Not kept for longer than necessary;
- Processed in accordance with appropriate security and within the data subject's rights;

The school must honour a data subject's right to (where applicable and lawful)

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them;
- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

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;

- Keep appropriate records around data processing, subject access requests and 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 this policy and the policies and procedures listed at the beginning of this policy.

Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate. They should also be aware of the importance of reporting any data breach in accordance with the School's Data Breach Procedure.

Staff should be aware of the rights set out above, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. Staff should therefore record every document or email in a form that would be appropriate if a data subject were to request access to it.

Staff should remain mindful of the Data Protection Principles above and the need for Data Security. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access. They should also comply with the guidelines in the policies on Remote Working and the Bring Your Own Device policies.

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:

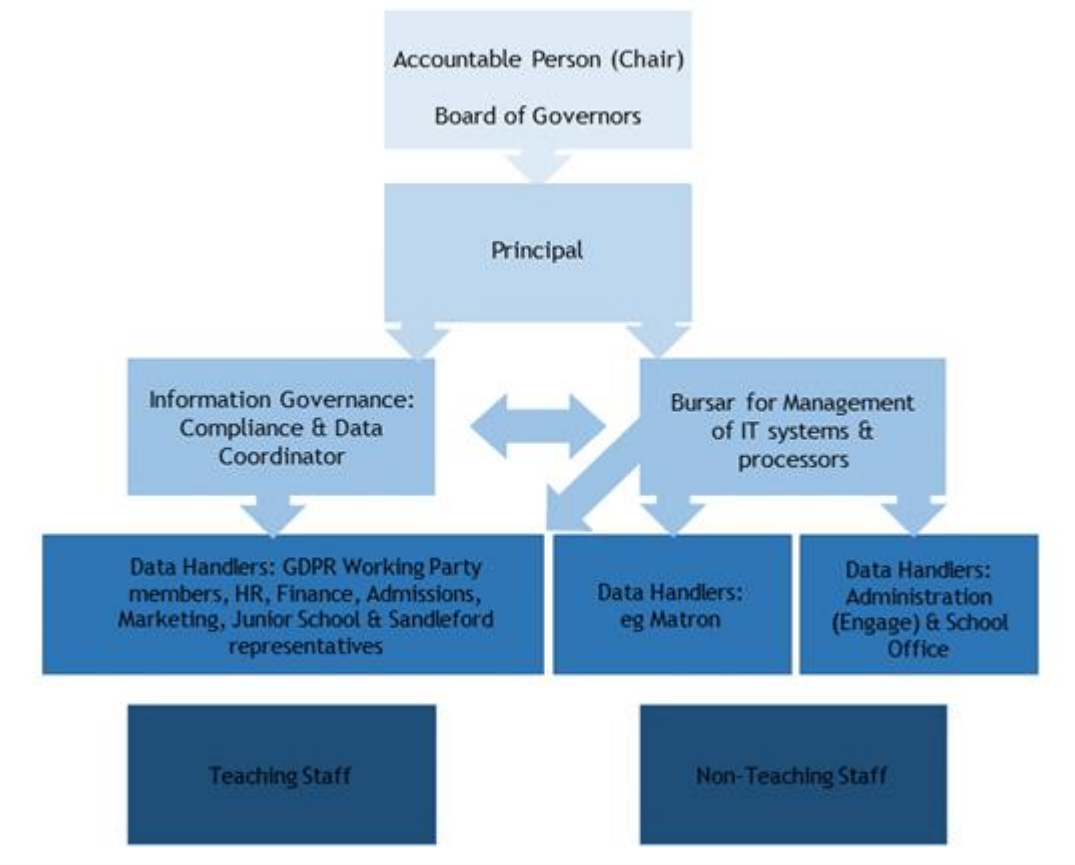
- Processing special category data or criminal offence data on a large scale.
- Using new technologies;
- Processing biometric or genetic data;
- Processing personal data in a way which involves tracking individuals' online or offline location or behaviour;
- Processing children's personal data for profiling 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
January 2020	Data Protection Act 2018 included Definition of Data to include "Living Individual" Definition of Data Breach added GDPR Principles amended to reflect wording in latest guidance from ICO Data subject rights added

Appendix 1- Data Protection Impact Assessment- Please complete and return to Data Coordinator

Date	_____	**Raised by**	_____
Please give details of the new data. **Describe the purposes of the processing.**			
Which data will be involved? E.g. staff medical details, pupils' external examination results. How many individuals will be affected?			
Will any of this data be "sensitive" or "biometric" data? Does any of the data come from children or another vulnerable person?	If yes, give details	Please give details of the source of this data, e.g. from registration or application form.	l
Is the individual aware you hold this data? What is your relationship with this individual?		Will this data be shared with anyone else, please give details?	
Give details of the intended processing of this data			
How will this data be used? What do we want to achieve? What is the intended effect on individuals? What are the benefits of the processing?		Please details of the anticipated retention period for this data. Will the data ever be archived or destroyed?	
Will this data ever be transferred to a country outside the EEA?		How will this data be held securely? Are any new technologies involved?	
Describe any potential risks of processing this data to the rights and freedoms of the individual.			
Does the individual have control over this data and would they expect you to use their data in this way?		Does this processing create a "data processor?" Is there a GDPR compliant agreement in place?	
Please give details of any necessary consultation with the stakeholders for this processing or with others within the school, e.g data individuals, HODS, JLT, SLT, Exec.			

To be completed by Data Coordinator and raised with Data Working Group as necessary. DPIA Number _____ Date received _____			
Does the processing actually achieve our purposes? Is there another way to achieve the same outcome?		How will we ensure data quality and data minimisation?	
What information will we give individuals? How will support their rights?		Data Handler for this data.	
Give details of any actions taken to minimise potential risks to rights and freedoms of individuals.			
Legal basis for holding this data		Date added to Data Register	

This DPIA to be retained by Data Controller as part of the School's Data Register.