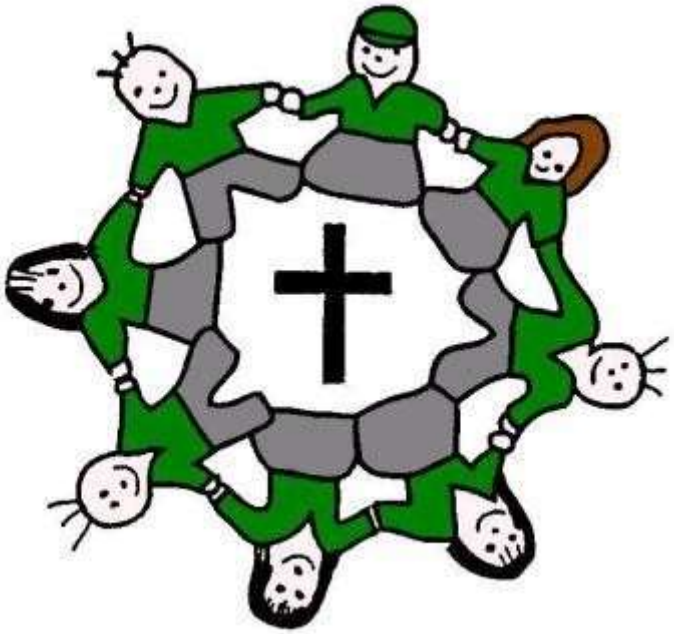
St Martin's CE Primary School



Data Sharing Policy

Version 1
September 2021

1. Objectives

1.1. We recognise the need for legal compliance and accountability and endorse the importance of the integrity, availability, confidentiality, resilience and security arrangements to safeguard personal data. We also recognise that there are times that personal data is shared with, and/or received from, other organisations and that this needs to be in accordance with data protection, human rights, duty of confidentiality and ethical considerations.

1.2. This policy sets out the key obligations and accountability in relation to data sharing to which we are fully committed.

2. Scope

2.1. In order to fulfil our statutory and operational obligations we have to collect, use, receive and share personal, special personal and crime data about living people, eg,

- Pupils and their families
- current, past, prospective employees
- clients and customers
- contractors and suppliers
- Governors

2.2. This policy covers all aspects of handling personal data, regardless of age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

2.3. This policy reflects the commitment to data protection compliance to both UK and EU legislation, in particular the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR).

2.4. Under data protection legislation it is important when sharing data to identify the roles of the parties involved, ie,

Data Controller: the body /individual that determines the purposes and means of processing the personal data. This can be alone or in conjunction with others.

Data Processor: the body /individuals who processes the data on behalf of and in accordance with the data controller's instructions.

Third Party: anybody who is not authorised to process the data by the data controller, the data processor or data subject.

Recipient: anybody to whom the data is disclosed, even if they are a third party.

2.5 Data sharing may mean the disclosure of data from one organisation to another or from one part of the organisation to another. Data sharing, may be for e.g.:

- a reciprocal exchange of data

- one or more organisations providing data to a third party or parties
- several organisations pooling information and making it available to each other
- several organisations pooling information and making it available to a third party or parties
- exceptional, one-off disclosures of data in unexpected or emergency situations
- different parts of the same organisation making data available to each other
- sharing with third parties for the delivery of services
- matching and/or profiling of data

3. Policy

3.1 When determining whether or not to share/disclose personal data, a DPIA may assist in the assessment of risks to privacy for the individual, and potential reputational and financial impact on the school in the event of inappropriate and unauthorised sharing/access to the data.

3.2 It is essential to establish:

- if using a data processor, is there a contract in place?
- is a data sharing agreement needed to set out clearly the parameters of the processing?

3.3 When using a data processor to act on our behalf when processing personal data, they are equally liable under data protection for any breaches of the law. It is a legal requirement to have a contract in place between parties that clearly sets out the roles, responsibilities and liabilities of each party and the parameters of the processing. See Appendix I for a data processor overview.

3.4 If the sharing is between data controllers, or when data controllers are acting jointly, i.e. not in a contractual relationship, then a data sharing agreement will serve the same purpose in setting out the roles, responsibilities and liabilities of each party and the parameters of the sharing.

3.5 In summary the considerations to be set out include:

- Is a data Privacy Impact Assessment required (DPIA)?
- the objective of data sharing
- express and implied statutory powers
- the lawful basis for sharing
- applicable exemptions to data protection principles
- how people will be informed of the use of their data
- the minimum data required for the purpose
- who will access/process the data

- how will it be stored/transferred
- the security controls and the upholding of any duty of confidentiality
- records retention
- ethical and human rights considerations
- the risks to the information and mitigation
- arrangements for managing individual rights
- arrangement for management security breaches
- review period for the agreement/contract

3.6 There are circumstances when the law allows data sharing/processing without full compliance with the data protection principles and/or without an individual's consent. These are not blanket exemptions and assessment needs to be made on a case by case basis. Examples of key exemptions that support this include, but are not limited to:

- crime and Taxation/protection of public funds
- legal professional privilege/legal proceeding, disclosure by law
- self-incrimination
- corporate finance/management forecasts
- negotiations
- confidential references
- regulatory functions of certain bodies
- protection of the rights of others
- exam scripts and exam marks
- research and statistics
- archiving in the public interest
- serious harm
- child abuse data
- law enforcement purposes of competent authorities

3.7 Where a request for personal data disclosure is received eg, from the police, enforcement agencies, or any other third parties, the request will need to be in writing. The request will need to set out why the disclosure is necessary ie, lawful basis and/or exemptions. A record will be kept of disclosures.

3.9 We may share personal data without an individual's knowledge or consent at the request of other organisations or proactively where it is required by Law, where it is necessary in an emergency situation, to identify and assist vulnerable people or where it is necessary in the interests of safeguarding vulnerable children and adults.

4. Assessment and Monitoring

4.1. An assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

4.2. Reports will be submitted to the Board of Governors.

5. Responsibilities and Approvals

5.1. Governing Body:

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2. Headteacher:

The Headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for the approval of this policy.

5.3. Data Protection Officer:

The Data Protection Officer will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

5.4. Governors/Employees:

All Governors and staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day to day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence.

Appendix I – Data Processor overview

A data processor contract must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions;
- the duty of confidence;
- appropriate security measures;
- using sub-processors;
- data subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

What responsibilities and liabilities do controllers have when using a processor?

Controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet GDPR requirements and protect data subjects' rights.

Controllers are primarily responsible for overall compliance with the GDPR, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

What responsibilities and liabilities do processors have in their own right?

In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the GDPR. If a processor fails to meet its obligations, or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract must offer an equivalent level of protection for the personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.