St Martin's CE (Aided) Primary School

East End, Newbury, Berkshire RG20 0AF

Telephone: 01635 597796

E-mail: adminoffice@st-martins.hants.sch.uk

Headteacher: Mrs K Bartlett

Data Protection Policy
Including Privacy Notices and
Procedure for Managing a Data Breach

Status: Draft / Final

Date policy produced/reviewed: 24.05.18

Policy produced/reviewed by: Headteacher

Ratified by the PayPerFin committee of the governing body: 29.06.18

Signed:

Position:

Date of next review: May 2020

St Martin's CE (Aided) Primary School
Data Protection Policy

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, who may be contacted at adminoffice@st-martins.hants.sch.uk.

The school issues Privacy Notices (also known as Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

Purpose
The purpose of this policy is to set out how St Martin's CE (Aided) Primary School deals with personal information correctly and securely and in accordance with GDPR and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

Scope
All school staff and governors involved in the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

Related policies and documents:
Confidentiality Policy
Complaints Policy
Child Protection Policy
Health and Safety Policy

What is Personal Information/Data?
Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles
The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. personal data shall be processed lawfully, fairly and in a transparent manner;
2. personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes);
3. personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;
4. personal data shall be accurate and, where necessary, kept up to date;
5. personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
6. personal data shall be processed in a manner that ensures appropriate security of the person.

Duties
Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment
St Martin's CE (Aided) Primary School is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- inform individuals of the identity and contact details of the Data Controller;
- inform individuals of the contact details of the Data Protection Officer;
- inform individuals of the purposes that personal information is being collected and the basis for this;
- inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this;
- if the school plans to transfer personal data outside the EEA, the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information;
- inform individuals of their data subject rights;
- inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point;
- provide details of the length of time an individual's data will be kept;
- should the school decide to use an individual's personal data for a different reason to that for which it was originally collected, the school shall inform the individual and where necessary seek consent;
- check the accuracy of the information it holds and review it at regular intervals;
- ensure that only authorised personnel have access to the personal information, whatever medium (paper or electronic) it is stored in;
- ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- ensure that personal information is not retained longer than it is needed;
- ensure that when information is destroyed, that it is done so appropriately and securely;
- share personal information with others only when it is legally appropriate to do so;
- comply with the duty to respond to requests for access to personal information (known as Subject Access Requests);
- ensure that personal information is not transferred outside the EEA without the appropriate safeguards;
- ensure all staff and governors are aware of and understand this policy and its procedures.

Complaints
Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk.

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Data Protection Officer, Headteacher or nominated representative.

Contacts
If you have any enquires in relation to this policy, please contact the Data Protection Officer or Headteacher, through the school office.

Privacy Notice
(How we use pupil information)

St Martin's CE (Aided) Primary School is committed to protecting the personal data of our children and their families. This policy sets out how we use any personal information that we hold. We will keep this information secure and will fully comply with all applicable UK Data Protection Act and all applicable consumer legislation.

Why do we collect and use personal information?

We collect and use personal information:

- to support children's learning;
- to monitor and report on pupil progress;
- to ensure the welfare of our children and provide pastoral care;
- to assess the quality of our services and how well our school is doing;
- to inform statistical forecasting and planning;
- to communicate with parents, carers and the school community about relevant information and events;
- to comply with the law regarding data sharing.

The categories of personal information that we collect, hold and share include:

- personal information (such as name, unique pupil number and address);
- characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- attendance information (such as sessions attended, number of absences and absence reasons) and exclusions;
- assessment information;
- modes of travel;
- relevant medical, special educational needs and behavioural information.

The General Data Protection Regulation allows us to collect and use pupil information with consent of the data subject, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of a data subject or another person and where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. When the personal information is Special Category Information we may rely on processing being in the substantial public interest in addition to consent of the data subject and the vital interests of the data subject or another.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Children Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010.

Collecting personal information

Whilst the majority of personal information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. Where we are using your personal information only on the basis of your permission you may ask us to stop processing this personal information at any time.

Storing personal data

We hold pupil data for and in accordance with our retention schedule from Hampshire County Council.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupils attend after leaving us;
- our local authority;
- the Department for Education (DfE);
- outside agencies providing support to our children including the school nursing service, children's services, educational psychologists, advisory teachers;
- data processors who provide school services such as email and text message communication.

Why we share pupil information
We do not share personal information with anyone without consent unless the law and our policies allow us to do so. We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to **https://www.gov.uk/education/data-collection-and-censuses-for-schools**.

To find out more about the NPD, go to **https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information**.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested;
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: **https://www.gov.uk/government/publications/national-pupil-database-requests-received**

To contact DfE: **https://www.gov.uk/contact-dfe**

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact our Data Protection Officer, through the school office.

You also have the right, subject to some limitations to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at **https://ico.org.uk/concerns/**

Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer or the Headteacher, through the school office.

Privacy Notice
(How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number, address, emergency contact details, relevant medical information);
- special categories of data including characteristics information such as gender, age, ethnic group;
- contract information (such as start dates, hours worked, post, roles and salary information) ;
- work absence information (such as number of absences and reasons);
- qualifications (and, where relevant, subjects taught).

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed;
- inform the development of recruitment and retention policies;
- enable individuals to be paid.

The lawful basis on which we process this information

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Children Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for and in accordance with our retention schedule from Hampshire County Council.

Who we share this information with

We routinely share this information with:

- our local authority;
- the Department for Education (DfE).

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to **https://www.gov.uk/education/data-collection-and-censuses-for-schools.**

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance.

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested;
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: **https://www.gov.uk/contact-dfe**

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Data Protection Officer, through the school office.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at **https://ico.org.uk/concerns/**

Contact
If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer or the Headteacher, through the school office.

Procedure for Managing a Data Breach

To be read in conjunction with the School Emergency Plan and Business Contingency Plan.

Background
Data security breaches are increasingly common occurrences, whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. St Martin's CE (Aided) Primary School needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

Aim
The aim of this procedure is to standardise the response to any reported data breach incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines.
By adopting a standardised consistent approach to all reported incidents it aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated;
- incidents are handled by appropriately authorised and skilled personnel;
- appropriate levels of school management are involved in response management;
- incidents are recorded and documented;
- the impact of the incidents are understood and action is taken to prevent further damage;
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny;
- external bodies or data subjects are informed as required;
- the incidents are dealt with in a timely manner and normal operations restored;
- the incidents are reviewed to identify improvements in policies and procedures.

Definition
A data security breach is considered to be "any loss of, or unauthorised access to, school data".
Examples of data security breaches may include:

- loss or theft of data or equipment on which data is stored;
- unauthorised access to confidential or highly confidential school data;
- equipment failure;
- human error;
- unforeseen circumstances such as a fire or flood;
- hacking attack;
- 'blagging' offences where information is obtained by deceit.

For the purposes of this policy, data security breaches include both confirmed and suspected incidents.

Scope
This procedure applies to all school information, regardless of format, and is applicable to all staff, pupils, visitors, contractors and data processors acting on behalf of the school. It is to be read in conjunction with the School Emergency Plan and Business Contingency Plan.

Responsibilities

Governors
The Governing Body is responsible for ensuring compliance with GDPR and monitoring the implication of the Data Protection Policy.

Senior Leadership Team
The Senior Leadership Team is responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required. The Senior Leadership Team will be responsible for overseeing management of the breach in accordance with approved procedure. Suitable delegation may be appropriate in some circumstances.

Data Protection Officer
The Data Protection Officer is responsible for advising the Senior Leadership Team and all staff about their data obligations, monitoring compliance, including managing internal data protection activities, training and conducting internal audits.

Information Users
All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Data Classification
Data security breaches will vary in impact and risk, depending on the content and the quantity of the data involved, therefore it is important that the school is able to quickly identify the type of the data and respond to all reported incidents in a timely and thorough manner.

Data Security Breach Reporting
Confirmed or suspected data security breaches should be reported promptly to the Data Protection Officer and the Headteacher. The actions identified in the School Emergency Plan and Business Contingency Plan should then be followed.

Any serious data breach, which interferes with the rights and freedoms of the data subject for which the controller is responsible, will be reported to the Information Commissioner within 72 hours of the breach.