DATA PROTECTION POLICY

ST MARY'S LEWISHAM CE PRIMARY SCHOOL

Our Vision

To be a learning community that promotes the unique gifts, wellbeing and potential of every person. Our work is founded on the life and teaching of Jesus Christ, building on His message of equality, peace and justice, guided by His words *'As I have loved you, so you must love one another' (John 13:34).*

Date created: 26.03.2018
Date Published: 26.03.2018

Introduction

St Mary's CE School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the school. This information is gathered in order to enable us to provide educational and other associated services. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

In collecting, processing, sharing and disposing of personal information relating to living individuals, St Mary's CE School is bound by the General Data Protection Regulation 2016.

The Information Commissioner's Office enforces the Regulation, issues relevant guidance and registers personal data sets held by any organisation.

As a data controller, St Mary's CE School must register itself with the Information Commissioners Office (ICO) annually.

This document sets out the school's policy for compliance with the General Data Protection Regulation (GDPR).

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation 2016, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

The Six Guiding Principles

The General Data Protection Regulation 2016 establishes six enforceable principles and St Mary's CE School as a registered Data Controller under the Act, will comply with these principles below:

1 Personal data shall be processed lawfully, fairly and in transparently in relation to the data subject.

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.

3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6 Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Act creates a single framework for access to personal information about living individuals held in both paper and electronic form.

See Schools guidance on what to do when a Subject Access Request (SAR) is received.

1. Differences in data sets

Personal and Special Categories data is any information – held manually or electronically – which relates directly to a living indivdual.

Personal Data-
This can include but is not limited to:

- Name and Address
- Contact Number
- E-mail address
- Date of Birth

Special Categories of Data-
This includes data under the following headings:

- Race or ethnic origin
- Political opinion/s
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Genetic and Biometric data
- The commission or alleged commission of offences, court sentences or allegations under investigation

While not legally special category of data the following should be given special consideration whilst processing

- Qualifications
- Income level
- Employment history
- Bank Details

.

2. Roles and Responsibilities

Head Teacher

- Responsible for ensuring all senior staff and the school are compliant with the General Data Protection Regulation

Data Protection Officer

- Must be in a position to undertake their tasks independently – report to Head Teacher directly
- Be point of contact for public for data protection issues
- Be involved in timely manner in all data protection issues
- Inform and advise the school, processors and employees of obligations
- Monitor data protection compliance
- Advise as required on Data Protection Impact Assessments
- To co-operate with supervisory authority, Information Commissioner's Authority (ICO)
- To act as contact point for the supervisory authority (ICO)
- Have due regard to the risk associated with processing, taking account of nature, scope and context of processing.

School Business Manager

- Maintaining the notification of registration for St Mary's CE School with the Information Commissioner's Office on an annual basis

Head Teacher & School Business Manager

- Providing guidance to ensure all staff are aware of their data protection responsibilities under the act
- Responsible for managing and reporting data breaches to the schools data protection advisor
- Providing guidance to process Subject Access Requests and Freedom of Information requests

- Ensuring appropriate and adequate training is available to staff

- Ensuring staff are compliant with this policy and any associated procedures

All Staff

- All staff have a responsibility to abide by the principles of the Data Protection Act. Any breach of this policy could lead to disciplinary action being taken.

3. Processing Personal Data

Employees of St Mary's CE School, when working with personal data, will adhere to the following:

- Only collect data necessary to carry out the purpose that the task relates to.

- Respond to requests for access to personal data within 30 calendar days (See Schools Guidance).

- Treat all personal information with equal respect for confidentiality and security whether in written, spoken or electronic form.

- Share of personal or sensitive data with informed consent. Where appropriate, the school may share information without consent if, in the school's judgement, there is a good reason to do so, such as the safety and well-being of the child/children involve and others who may affected.

- Only use third parties to collect and process school's data where appropriate sharing agreements are in place, ensuring the protection of the data.

- Only retain personal data for a specified time period defined by the Schools Retention Schedule. (See specific schools guidance on retention)

- Not delay data sharing where it is necessary to protect the vital interests of any individual.

- Seek approval from senior management before disclosing information for research purposes.

4. Privacy Notices

Principle 1 of the General Data Protection Regulation states that all personal data will be processed fairly, lawfully and transparently and Principle 2 states that personal data shall be obtained for specified, explicit and legitimate purposes.

St Mary's CE School is commited to processing personal data fairly and lawfully and have a written Fair Processing statement/Privacy Notice visible and easily accessible

on the school's website explaining to individuals how St Mary's CE School will process their data.

Having this statement/notice publicy available means that any individual will be able to read it before completing a data collection form (paper or electronic), and therefore will know exactly why the data is being collected and for what specific purpose/s.

The Privacy Notice includes the identity of the data controller (the school), what the data is being used for, whether the data will or may be used for any other purposes, and any extra information which will help the individual to understand how their data is used in line with data protection. The Privacy Notice should be provided the time the information is obtained from the individual if it's collected directly from the data subject. If it isn't collected directly from the data subject then it should be provided within a reasonable period of having obtained the information (maximum one month). If the information is used to communicate with the data subject, the latest it can be is when the first communication takes place. If disclosure to another party was unforeseen, then the Privacy Notice must be provided before the information is disclosed. If personal data is processed for a new reason/purpose at a later date an updated Privacy Notice must be provided.

In general terms, a Privacy Notice should tell individuals the following about the school:

- Who we are
- Where we are based in the UK
- What we are going to use their data for and legal basis for doing so
- Who we will share individual's data with (if anyone or a third party)
- Individuals Rights to accessing their own data including the fact that the Data Subject can complain to The Information Commissioner
- How we will keep individuals data secure and protected
- Identity & contact details of the School's Data Protection Officer
- The retention period for the data
- Any legal or contractual requirement to provide the information; plus the impact of not providing the data
- Automated decision making, with information about the consequences

A Privacy Notice should be genuinely informative and clear enough for children to understand so the school can be transparent and give individuals reassurance that they can trust the school with their personal data.

5. Information Sharing

St Mary's CE School understands that it is most important that people remain confident that their personal information is kept safe and secure, and that the school maintain the privacy of the individual, whilst sharing information to deliver better

services. It is therefore important that the school can share information appropriately as part of their day-to-day practice while protecting data when sharing.

Third Party organisations must follow the specific Information Sharing Agreements (ISAs) set out by St Mary's CE School when sharing data. ISAs provide a framework for the secure and confidential obtaining, holding, recording, storing and sharing of information between the school and third parties.

Robust IT security systems and measures must be in place to protect the school's electronic data and its IT infrastructure from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Please refer to the school's ISAs for protocols on information sharing.
See IT security policy for protecting information electronically and the records management policy for handling paper documentation.

6. Information Requests

There are two different information requests:

- **Subject Access Requests (SARs)**

Individuals have the right to ask for access to their information which can include factual information, expressions of opinion, and the intentions of the school in relation to them, irrespective of when the information was recorded.

There are two distinct rights of access to the information schools hold about pupils:

- **Right to the educational record**
  Under the Education (Pupil Information) (England) Regulations 2005, a parent or legal guardian has the right to access their child's educational record.
- **Subject access right**
  Under the General Data Protection Regulation 2016, a pupil has a right to see their own information. A parent or legal guardian may also make a request on behalf of their child.

If a pupil or parent makes a request for educational records, the school must respond within 15 school days. Fees for these requests will depend on the number of pages of information supplied. (For more information ask at the schools business manager)

If a pupil or parent makes a subject access request for personal information, the school must respond promptly and at most within 30 calendar days. Schools will be unable to charge for most Subject Access Requests

Requests made containing both educational and personal records, will be dealt as stated above: the educational part within 15 school days and personal within 40 calendar days.

See Subject Access Request guidance for details.

(For help and advice in responding to a Subject Access Request, contact the schools data protection Advisor)

• Freedom of Information Requests (FOI's)

The Freedom of Information Act 2000 (FOIA) provides public access to information held by schools. It does this in two ways: schools are obliged to publish certain information about their activities; and. members of the public are entitled to request information from schools.

St Mary's CE School will comply with Freedom of Information requests and release non personal and non confidential information held by the school, after applying any relevant exemptions to protect certain categories of data.

The Act requires that all requests must be in writing (to include letters, faxes and e-mails). Requests must state clearly what information is required and must provide the name of the person with an address for correspondence.

On receipt of a FOI request, a school must respond promptly and in any event within 20 working days.

See Freedom of Information guidance for details.

(For help and advice in responding to an FOI request, contact the schools data protection advisor)

• Appeals & Role of the ICO

In the event of a complaint or challenge regarding an information request response, whether this is a SAR or an FOI, the initial request, decision audit trail, correspondence and information released will be reviewed.

If the requestor is dissatisfied with the appeal outcome they may seek an independent review by the Information Commissioner.

The Information Commissioner is an independent official appointed by the Crown to oversee the General Data Protection Regulationand has the authority to demand disclosure.

In the first instance however the Information Commissioner will usually expect that individuals will have taken the matter up first with the School.

St Mary's CE School will comply with all notices and guidance issued by the Information Commissioner.

7. Rights of Individuals

Individuals also have the right to:

- Have personal data rectified if it is inaccurate or incomplete.
- Request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Request the suppression of processing of personal data
- Move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability
- Object to processing of data unless you can demonstrate compelling legitimate grounds for the processing
- Object to automated individual decision-making, including profiling

8. Dealing with breaches of the GDPR

St Mary's CE School holds personal and sensitive data relating to employees, children and their families.

Every care must be taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

What is a data breach?

Inadvertent breaches of confidentiality can occur. The following are examples and not limited to;

- Reading confidential files when there is no requirement to do so
- Giving excessive information out when less would suffice
- Sending information in error eg.to a wrong email address
- Files/records removed from the office and lost
- Unencrypted devices used and lost containing personal/sensitive details
- Information that hasn't been redacted correctly before publishing

Known breaches in confidentiality must be reported to the Headteacher/SBM immediately so it can be recorded and a formal investigation carried out.

What to do when a breach occurs:

There are four elements in dealing with a data breach. These are:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

See the schools Data Breach Process for more information in the event of a data breach.

9. Training

St Mary's CE School will arrange training for all staff so they are fully aware of their obligations and responsibilities under the Data Protection Act.

10. Confidentiality

St Mary's CE School must ensure that all personal data is treated confidentially. All staff must comply with the Schools Data Protection Policy, Information Security Policy, Records Management Policy, Subject Access Request Process, Freedom of Information Request Process and Data Breach Process.

11. What happens if this policy is breached?

Failure to adhere to this or any related policy, could lead to disciplinary action.

12. Policy Authorisation

Name/Role	Date	Version
Melissa Barrett Data Protection Adviser for Schools	28.07.2016	V 1
Gemma Varela & Samuel Akeredolu Senior Customer Information Officers Data Protection Advisers for Schools	08/03/2017	V 2
Gemma Varela Data Protection Officer for Council & Schools	10/05/2017	V 3
Brendan Myles Data Protection Officer for Council & Schools	16/03/2018	V 4