St Mary & St Paul's CE Primary School

Data Protection Policy

Version:	1
Ratified by:	Governors
Date ratified:	May 2019
Name of organisation/author:	Knowsley LA
Name of responsible committee/individual:	P Brooksbank
Date issued:	
Review date:	May 2020
Target audience:	All employees

Introduction

1.1 The Data Protection Act 1998 (DPA) has been replaced by the General Data Protection Regulation (GDPR). The GDPR builds on the principles and the themes of the DPA and establishes a framework of duties for the School and rights for individuals, that aim to keep personal information safe. The GDPR encourages a balance between the individual's right to privacy and an organisation's need to conduct legitimate and appropriate operations with personal data.

1.2 **St Mary & St Paul's CE Primary** is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the GDPR. The school has established the following policy to support this commitment. It is the **personal responsibility** of all employees (temporary or permanent), Governors, contractors, agents, volunteers and anyone else processing information on our behalf to comply with this policy.

1.3 Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990, the GDPR or the Data Protection Bill. All incidents will be investigated and action may be taken under the school's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken.

1.4 This policy explains what our expectations are when processing personal information. This policy should be read together with Information Security Acceptable Use Policy, and the School Records Retention and Disposal Schedule.

1. The Data Protection Principles and Definitions

1.1 The GDPR is concerned with the use (processing) of personal data.

Personal data is information that either on its own, or when combined with other information, can be used to identify a living individual.

Examples of personal data include: - names, addresses, dates of birth, photographs, IP Addresses, Vehicle Registration Plates, CCTV footage.

The GDPR also defines personal information that is more sensitive and must be treated with a higher level of privacy and respect. This is called Special Category Data.

Special Category Data is any data that falls into the following categories: - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data such as fingerprints, sexual history or sexual orientation, any data relating to physical or mental health conditions.

Processing Data is referred to throughout the GDPR and data protection legislation. This means any use of the personal information. This includes collecting, disclosing, destroying, archiving and organising.

Data Subject is the person who the personal data is about. For example, the children named on a class register at a school are all data subjects of that register.

Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The School itself is a Data Controller as it chooses how it collects, uses and shares its own data.

The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act or the GDPR. This means they can issue: -

- An Undertaking which commits an organisation to improving their Data Protection practices.
- An Enforcement Notice ordering that an organisation does something specific e.g. train all staff to a high standard.
- A Monetary Penalty for serious and significant breaches. Under the Data Protection Act, this can be anything up to £500,000. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's global turnover.

1.2 The Principles

The GDPR contains a number of Principles that must be met in order to use personal data in line with the law.

Personal Data must be: -

1. Processed Fairly, Lawfully and Transparently
2. Processed for a Specified and Legitimate Purpose
3. Adequate, Relevant and limited to what is relevant
4. Accurate and up to date
5. Kept no longer than necessary
6. Stored securely using technical and organisational measures

Principle One – Fair, Lawful and Transparent

Fair and Transparent

When the school collects personal information from an individual, we must inform them of what we intend to do with that information once we have it. This is called a Privacy Notice.

The Privacy Notice must include the following information: -

- Who will own the data (normallythe school)
- What the information will be used for
- The legal basis for collecting and using the information
- Who the information will be shared with
- How long the information must be kept for and how it will be stored
- What Rights under the GDPR that the data subject has
- How they can complain
- How they can complain to the Information Commissioner's Office
- Whether the data is stored outside of the UK
- Whether any automated decisions are made using the information

The Privacy Notice must be given to the data subject as soon as possible when collecting their information and this can be done online, through the post or in the form of a recorded voice message. As long as the Privacy Notice is provided, it can take any form necessary.

Lawful

To use information lawfully, the School must ensure that no laws are broken when processing the data. This means we cannot use data to break any other laws within the UK or Europe.

As well as this, the School must meet what is called a condition for processing when using the information. The conditions for processing are explained below.

The School can use information if we can meet one of the following conditions:-

- The data subject has consented to their information being used. This consent must be specific, informed and freely given. The data subject must know what they are consenting to and be given a genuine choice, before consent can be classed as appropriately obtained.

- The personal data is being used to perform a contract with the data subject or to undertake actions necessary for creating a contract with the data subject.

- The personal data has to be processed because legislation says that the School has to. This also applies when the School receives a court order that demands disclosure of information.

- The personal data is used in line with the vital interests of the data subject. This is usual a life or death situation.

- The personal data is used in line with a public function or legal power that the School is meeting. For example, the Children's Act 1989 gives

the School the power to look after children at risk of harm. This power also allows the School to use information to complete this function.

If the School wishes to use Special Category (Sensitive) Data as categorised above, they must meet one of the above conditions and one from the list below: -

- The School has obtained explicit consent from the data subject. This means that they have been explicitly told everything that will happen with their sensitive data once it has been given to the School.

- The processing is necessary for the School's obligations of employment law or social security.

- The use of information is in the vital interests of the data subject. As above, this is a life or death situation.

- The use of information is necessary for the legitimate aims of a political party, religious group or similar not for profit organisation such as a trade union.

- The personal information has been made public deliberately by the data subject

- The use of the information is necessary for pursuing or defending a legal claim or whenever the courts need to use data.

- The use of data is necessary and in the public interest when a public authority is acting using a legal power written into law. This is the same as the public function condition in the list above. It is also known as a "legal gateway".

- The use of the data is necessary for the purposes of preventative or occupational medicine, this also includes the provision of social care.

- The use of the data is necessary for public health purposes such as the prevention of serious diseases or handling cross-border health issues such as pandemics.

- The use of information is for archiving purposes such as historical archiving or scientific research in the public interest.

Principle 2 – Specified and Legitimate Purpose

The School must only use, collect and share information for a specified and legitimate purpose. This purpose must be in line with the School's aims and values and not contradict any laws or moral obligations.

Once we have collected information for a specific purpose, we must only use that information for purposes compatible with the original aim.

For example, if the School collects information for a social care purpose, we can use it for other social care purposes such as evaluating the quality of the social care provided. However, we couldn't use social care information to inform school trip planning as this is not a compatible purpose because it so different to the original purpose for collecting the information.

Principle 3 – Adequate, Relevant and limited to what is necessary

The School must only use, collect or share the information that we need in order to complete the purpose we are trying to achieve. For example, if the School only needs to collect a name and address in order to complete the purpose, only then only the name and address should be collected.

Principle 4 – Accurate and up to date

The School must ensure that all of its information is as accurate as possible. This means that if we find out something new about a data subject such as a change of address, School systems are updated as soon as possible to reflect this change.

Inaccurate information can lead to breaches, such as letters or emails being sent to wrong recipients or the wrong decisions being made about people on the back of inaccurate information.

Principle 5 – Kept No Longer Than Necessary

The School has a responsibility to ensure that information is retained for the correct amount of time, and no longer. All of the School's information has a date by which is should be securely deleted or archived. This is written into the School's Retention Schedule.

Principle 6 – Stored Securely

The School must take all appropriate technical and organisational measures to keep information secure and prevent it from being lost or put at risk of being seen by people who shouldn't have access to it.

This can take a variety of forms. Examples of technical and organisational measures can be found below.

Technical Measures

- Firewalls
- Anti-virus software
- Encryption
- Secure emails such as GCSX and Egress
- VPNs (Virtual Private Networks)

Organisational Measures

- Policies and Procedures in place to help staff understand their duties under data protection
- Training
- User guides on for staff
- A more knowledgeable and open culture towards Data Protection

The aim of employing technical and organisational measures is to help staff keep information securely. This is through giving them the technology and the knowledge to know how to safely handle information. In line with this, if you identify any further training or equipment needs for your team, contact your line manager so that they can be arranged.

2. Access and use of personal information

3.1 Access and use of personal information held by the School is only permitted to employees (temporary and permanent), Governors, contractors, agents, volunteers and anyone delegated access as part of their official duties.

School information is held on a need to know basis, meaning that unauthorised or inappropriate use of the information is strictly forbidden.

School employees must only access information that they have a professional and legitimate need to see. Just because an employee has access to a specific system does not mean that the employee has the right to access all records within that system. Employees must only access cases or files within their caseloads, or those that are directly relevant.

Any deliberate or malicious access to systems or records will be dealt with in line with the School's Disciplinary Procedures. There are also a range of criminal offences under the Computer Misuse Act 1990 and in Data Protection law for unauthorised use, obtaining or destruction of personal data. These offences can be punished by up to 12 months in prison or a fine of up to £1,000.

You have personal responsibility for the way you handle personal information as part of your day to day work. As a School employee, you are required to keep all information you use secure and confidential.

The general rule when using information is, treat the information with the respect that you expect your own personal information to be treated. All staff must ensure that their use of personal information is appropriate and respectful.

Handling and using personal data in line with the law is not complicated. The following tips are easy to follow, easy to implement and could make all the difference to your daily work in helping to avoid data breaches.

- Always lock your screen when you leave your desk. This avoids leaving your systems open to access and also stops those nearby reading any personal data you may have left onscreen.
- Clear documents away at the end of the day or when leaving your desk. This stops people who are walking past your desk from reading things they shouldn't.
- Always check for ID when holding doors open for people. It is everyone's responsibility to ensure the security of School buildings and make sure only authorised staff have access to them.
- Double check when entering information into School systems. Inaccurate information is the biggest cause of data breaches for the School. Taking the time to check addresses and phone numbers is a vital part of data handling.
- Double check addresses when sending emails. It is easy to mistype or click the wrong name on Outlook. Once the email has gone, it can't be retrieved. Take the time to get the recipient right before you press send.
- When taking information out of the office, think about the most appropriate way to do so. Are School tablets and laptops encrypted and difficult to access if they are lost? Paper documents are not secure as they can be read by anyone who finds them. If you don't need to print something, don't.
- If you are regularly sending personal information to organisations outside of the School, check that you have the means to send this information our securely.
- Take care when working from home. Your family members don't have a right to see the information you use for work.
- Don't leave equipment or documents in your car overnight if you need to take them home. You wouldn't leave your own laptop on the front seat of your car, so don't leave your work on there either.

Using School Systems

- Just because you have access to a system, this does not mean you have the right to access all of the information on it. Access is on a "need to know" basis.
- "Curiosity" checks are not permitted. You must have a genuine, legitimate work purpose to access information

- Never share passwords. If a colleague forgets their password, they need to have it reset. Do not let them access a system under your username.
- Any information you access on a system will be logged. Do not let colleagues use your computer to retrieve information and do not undertake requests on their behalf.

3. Disclosing personal information

4.1 Personal information must only be shared when the staff member receiving the information is satisfied as to the legal basis for sharing the information. School staff must ask appropriate questions to ensure the requester (whether internal staff or an external partner) has the appropriate legal reason to see the information they are requesting.

Where necessary, staff members are encouraged to speak to their line manager to ask advice, or contact the Data Protection Officer

4.2 If personal information is given to another organisation or person outside of the school, the disclosing person must identify their lawful basis for the disclosure (see section 4 above) and record their decision for sharing, along with the written request for information.

This should include;

- a description of the information given;
- the name of the person and organisation the information was given to;
- the date;
- the reason for the information being given; and
- the lawful basis.

4.3 If an Information Sharing Agreement (ISA) exists, this should be adhered to.

4.4 In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

4.5 When personal information is given internally or externally, it must be shared using a secure method. Secure email such as GCSX and Egress are preferred.

- Egress can securely deliver emails to any email address, including Hotmail or Googlemail accounts.
- GCSX accounts can deliver emails securely as long as the account receiving the email contains a suffix such as .GCSX, .PNN, .GSI or @NHS.net

4. Accuracy and relevance

4.1 It is the responsibility of the staff who receive personal information to make sure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate. If the information is found to be inaccurate, steps must be taken to correct it. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

5. Retention and disposal of information

5.1 **The School** holds a large amount of information. The GDPR requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.

6.2 The School Records Retention and Disposal Schedule must be checked before records are disposed of, to make sure that the retention period for the information in question, has been served.

6.3 For specific information regarding retention and disposal of personal data, consult the School's Data Protection Officer – **Paul Brooksbank.**

6. Rights of the Data Subject

7.1 Individuals have a number of Rights under the GDPR and they are able to enact them against any organisation at time they choose.

The Rights include: -

- **The Right of Subject Access** – the right to request a copy of data held about them by an organisation and find out how it is used.
- **The Right of Rectification** – the right to ask for inaccurate or incorrect information to be corrected or removed.
- **The Right of Data Portability** – the right to move data from one organisation to another. This could apply when moving bank accounts or energy suppliers.
- **The Right to Be Forgotten (Erasure)** – the right to ask for data to be removed by the organisation that holds it.
- **The Right of Restriction** – the right to stop information being used whilst a complaint is made.
- **The Right of Objection** – the right to ask an organisation to stop using their data. This is particularly used with regards to direct marketing.

7.2 The school has 30 days (one month) to respond to an individual's request to enact their Rights. This is provided the applicant has put their request in writing and suitable identification has been supplied.

7.3 Further information about the rights of the individual can be found in the School's Information Rights Policy.

Reporting security incidents

8.1 As a Data Controller (organisation that owns data), **St Mary & St Paul's** has a responsibility to monitor and investigate all incidents that occur within the organisation that involve any of the GDPR Principles being breached.

All incidents need to be identified immediately, reported using the Data Breach form. All incidents will be investigated by the Data Protection Officer.

Where an incident occurs, staff must inform the Data Protection Officer as soon as possible. The School has a responsibility to report all serious incidents to the Information Commissioner's Office within 72 hours of discovery.

Staff are advised to contain all incidents of data loss as quickly as possible, either by retrieving information sent in error, locking down erroneous access or asking accidental recipients of School data to confirm it has been deleted.

All relevant incidents and risks that are identified should be reported to the Data Protection Officer, regardless of how trivial they may seem. The School must constantly evaluate and improve its data protection and information security practices to address the new risks it uncovers. This is to stop breaches from occurring or reoccurring as the case may be.

8.2 Specific procedures have been developed for the reporting of all information security incidents and weaknesses. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken.

8.3 All employees (permanent, temporary and external users) must be aware of the procedures and obligations in place for reporting the different types of incidents and weaknesses which may have an impact on the security of the school's information assets.

9 Data Protection by Design

9.1 The School will meet the requirements of the GDPR by building data protection into all new projects from the start and employing appropriate technical and organisational measures to keep personal data secure. This will be achieved through completing Data Protection Impact Assessments (DPIAs)

9.2 All new projects must be subject to a DPIA before they can be put out to tender. This step is mandatory and must not be ignored.

9.3 A DPIA is a process of assessing the risks to privacy and to personal data in a project. A DPIA enables the School to identify risks and problems at an early stage in the project, meaning that changes can be made quickly and without incurring expenses.

10 Contact & Data Protection Officer (DPO)

St Mary & St Paul's has appointed a DPO in order to:

- Inform and advise **St Mary & St Paul's** and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor **St Mary & St Paul's** compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

The role of DPO will be carried out by the most appropriate member of staff within the school.

The DPO will operate independently, their role being to:

- advise the school and its employees about the obligations to comply with GDPR and other data protection requirements – this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights.
- monitor your school's compliance with GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits.
- act as the first point of contact with the Information Commissioner's Office and for individuals whose data you process.

Where advice and guidance offered by the DPO is rejected by the school, this will be independently recorded.

Advice offered by the DPO will only be declined at the direction of the Head and/or Governing body and will be provided to the DPO in writing.

The School's Data Protection Officer is available for advice and guidance regarding all aspects of data protection and GDPR. Please contact: -

Paul Brooksbank

St Mary & St Paul's CE Primary School
Bryer Road
Prescot
Merseyside
L35 5DN

0151 426 6869

To be reviewed May 2020