



St Joseph's RC Primary Data Protection Policy

Policy Date:	September 2021
Reviewed	12 th June 2024

Table of Contents

REVISION HISTORY	3
DOCUMENT APPROVAL	3
1.PURPOSE	4
2.SCOPE	4
3.RISK APPETITE	5
4. POLICY STATEMENT	5
4.1 Data Protection Regulations	5
4.2 The GDPR Data Protection Principles	6
4.2.1 Lawfulness, Fairness and Transparency.....	7
4.2.1.1 Lawful basis for processing personal data.....	7
4.2.1.2 Data Subject Consent Requirements	7
4.2.1.3 Special category data and explicit consent.....	7
4.2.1.4 Transparency.....	8
4.2.2 Purpose Limitation	8
4.2.3 Purpose Minimisation	9
4.2.4 Data Accuracy	9
4.2.5 Storage Limitation.....	9
4.2.5.1 Data Retention and Destruction	9
4.2.6 Integrity and confidentiality – Data Security	9
4.2.6.1 Access and Storage	9
4.2.6.2 Anonymisation Requirements	11
4.2.7 Accountability	11
4.2.7.1 Training	12
4.2.7.2 Documentation	12
4.2.7.3 Records of Processing	12
4.2.7.4 Use of Biometric Information	12
4.3 DATA PRIVACY BY DESIGN (AND DEFAULT)	12
4.3.1 Data Protection Impact Assessment (DPIA)	13
4.4 DATA SUBJECT RIGHTS	13
4.4.1 Subject Access Requests (SARs).....	14
4.5 DATA SHARING / THIRD PARTY PROCESSING	14


4.5.1 Sharing with Third Parties.....	14
4.5.2 Third Parties.....	15
4.5.3 Joint Controllers.....	16
4.6 DATA BREACHES.....	16
4.6.1 Complaint Handling Requirements.....	17
5 POLICY GOVERNANCE	17
6. DEFINITIONS.....	18

Revision History

The below table provides the revision history for this document. Each revision has an associated date, issue number, and description of the changes and/or content. The document revisions appear in descending order, with the most-recent iteration appearing first in the table.

Date	Description	Author
23/6/23	Policy review completed	Karen Latimer, Data2Action
18/08/2021	Final Approved Version	Karen Latimer, Data2Action
22/07/2021	Initial Draft	Karen Latimer, Data2Action

Document Approval

Document Name	Data Protection Policy	
Publication Date	September 2021	
Review date	June 2024	
Prepared by	Karen Latimer, Data2Action	
Approval	Paul Bradley Chair of Governors	

1. Purpose

The purpose of this Policy is to apply the principles of the Data Protection Regulations and to ensure all employees (including temporary, casual or agency staff) and contractors, consultants and suppliers working for, or on behalf of, St Joseph's Roman Catholic VA Primary School (the school) and who process personal data on behalf of the school, understand the requirement to comply with Data Protection Legislation. Personal data processed by the school includes that related to our students, parents/carers, employees, Governors, contractors and any other identifiable living individual.

The UK General Data Protection Regulation (GDPR) is implemented in the UK by the Data Protection Act 2018.

The school strives to ensure it delivers fair outcomes for students, parents/carers and employees and shall never knowingly or intentionally breach any applicable law or regulation relevant to the conduct of its activities. The school is committed to the highest standards of ethical conduct and integrity in its activities and is dedicated to acting in an open and honest manner. The school's employees and associated third parties should always comply with the spirit of this Policy, the overriding objective of which is to protect Personal Data held by the school.

This Policy does not contain an exhaustive set of requirements and should therefore be read in conjunction with the wider suite of data and information security policies which exist to provide a structure for employees to work within and remain compliant with all relevant legislation.

2. Scope

The school is required by law, and to perform its function, to collect and use certain types of personal information. This personal information must be dealt with lawfully and correctly whether it is collected, recorded and used on paper, information technology or other material. This includes information on current, past and prospective students and employees, suppliers, service users and others with whom it communicates with including:

- Personal data processed by the school.
- Personal data controlled by the school but processed by another third party, on the school's behalf (for example payroll provider).
- Personal data processed jointly by the school and its partners.

Personal data held by the school may be held in many forms including:

- Database records
- Computer files
- Emails
- Paper files
- CCTV and video recordings
- Sound recordings
- Photographs
- Website
- Mobile phones.

Data subjects may include:

- Current, past and prospective employees and students
- Parents and other pupil or staff contacts
- Governors
- Suppliers
- Service users
- Others with whom the school communicates.

This Policy also covers any employees or students who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities.

This Policy provides outlined measures and puts in place a structure for monitoring compliance.

3.Risk Appetite

The school has no appetite for regulatory breaches. The school has a very low risk appetite to breaches of this Policy and related procedures.

4. Policy Statement

4.1 Data Protection Regulations

At the time this Policy was written, it aims to satisfy data protection and associated regulations in the United Kingdom which include:

- The UK General Data Protection regulations (UK GDPR)
- The UK Data Protection Act 2018
- Privacy in Electronic Communications Regulations (PECR) 2003, updated in the e-privacy bill on 25th May 2018
- The Education Act 2011
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012

The UK General Data Protection Regulation (GDPR) governs how information about individuals should be treated. It also gives rights to individuals whose data is held. The Regulation applies to all personal data collected at any time whether held on computer or paper record.

This Policy will be updated in accordance with any changes made to the afore mentioned Regulations.

Data Processing in the UK is regulated by the Information Commissioners Office (ICO). The school is registered with the ICO as a Data Controller, registration Z6385348.

The school have appointed the following Data Protection Officer (DPO) who is the central point of contact for all **data protection related** matters on behalf of the school.

DPO: Sarah Burns

Company: Data2Action

Email: sarah.burns@data2action.co.uk

Telephone: 0203 9894592

Company Registered Address – Unit e2, Innovator House, Silverbriar, Sunderland, SR5 2TP.

4.2 The GDPR Data Protection Principles

There are seven key GDPR Data Protection principles relating to the processing of personal data which the school must comply with:

- 1. Lawfulness, Fairness and Transparency** – Data should be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- 2. Purpose Limitation** – Data should be collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes.
- 3. Data Minimisation** - Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 4. Accuracy** – Data should be accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purpose for which they are processed, are erased or rectified without delay.
- 5. Storage Limitation** – Data should 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 is processed.
- 6. Integrity and confidentiality** – data should 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.
- 7. Accountability** – the data controller must be responsible for and be able to demonstrate how it applies principles 1 to 6.

4.2.1 Lawfulness, Fairness and Transparency

4.2.1.1 Lawful basis for processing personal data

Processing of personal data is **only permitted** if one of the following applies;

- It is done with the expressed **consent** of the data subject.
- It is necessary for the provision of service or the performance of a **contract**.
- It is necessary for compliance with a **legal action**.
- It is necessary to protect the **vital interests** of the data subject or another natural person.
- It is necessary for the performance of a task carried out in the **public interest**.
- It is necessary for the purpose of the **legitimate interests**. When using the lawful basis of Legitimate Interest, a 'Legitimate Interest Assessment' (LIA) should be completed to ensure that the interest is demonstrable.

4.2.1.2 Data Subject Consent Requirements

Where processing is based on consent, the school must be able to demonstrate the data subject has consented to processing of personal data. Any consent must be freely given, which means that the school cannot make the provision of any services or other matter conditional on a **data subject** giving their consent.

In the UK, any person aged from 13 years old is deemed sufficiently literate to understand and enforce their data rights and therefore give their consent. At this age it is not the parent's consent but the child's that is generally required. It may be however that the child is not able to fully understand the context or extent of the consent and as such, it may be appropriate to also seek consent from the parent. For further support on this please refer to the DPO.

If the data subject's consent is given in the context of a written declaration, which also concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject must have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. A record must always be kept of any consent, including how and when it was obtained.

4.2.1.3 Special category data and explicit consent

Processing of data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership**, and the processing of **genetic data, biometric data** for the purpose of uniquely identifying a natural person, data concerning **health** or data concerning a natural persons **sex life or sexual orientation** is generally prohibited, but where this processing is vital, it must only be carried out with either the **explicit consent** of the data subject or in fulfilment of other conditions and set out in Article 9 of the regulation. A record of the explicit consent must be retained.

Special care must be taken as vulnerable or children with SEND may not be able to provide their explicit consent. Please refer to the DPO where this may be the case.

4.2.1.4 Transparency

The school outlines its obligation to inform data subjects via the Privacy Notice which is located on the school's website for external reference. Data subjects in the context of the school will include pupils, parents/guardians/carers, Governors and employees.

The Privacy Notice may also be provided where there is a specific activity which requires the collection and processing of personal data. Therefore, at the point where personal data relating to a data subject is collected, the school must, at the time of collecting the personal data, provide the data subject with the following information

- The identity and contact details of who is collecting the data e.g., the specific school.
- The contact details of the Data Protection Officer (DPO)
- The purposes of the processing as well as the legal basis for processing.
- The third-party recipients or categories of recipients.
- The period for which the personal data will be stored.
- The existence of the right for the data subject to:
 - Be informed
 - Request access to their data
 - Rectification
 - Erasure
 - Restrict processing
 - Object to processing
 - Data portability
 - the existence of any automated decision-making, including profiling, as well as the significance and the envisaged consequences
- The data subjects right to lodge a complaint with a supervisory authority (ICO)
- The lawful basis or processing
 - Where processing of data is based on consent, the existence of the data subjects right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. This is particularly relevant where a child's data is obtained where parental consent may have been obtained, the child has the right to withdraw this consent
 - Where the processing is based on legitimate interests, what the interest is

4.2.2 Purpose Limitation

The school and its employees must only collect and process personal data for the purpose specified at the point of collection. When the data is used for a purpose other than for which it was collected, the school must provide the data subject with confirmation of this, prior to any further processing.

4.2.3 Purpose Minimisation

The school will collect, process and create records containing personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements. Such processing or creation of records will:

- Enable employees to do their work consistently in full knowledge of the processes, decisions and actions that inform and drive the delivery of the teaching provision and associated services.
- Ensure the availability of credible and authoritative evidence to protect the rights of the school, its employees and students, parents and carers.
- Demonstrate accountability by providing the evidence and information required for any internal or external audit
- Ensure that all records are up to date and accurate
- Make sure that only relevant data is captured, and the personal data obtained is not excessive

4.2.4 Data Accuracy

Personal data processed by the school must be accurate and always kept up to date. All reasonable steps must be taken to ensure that personal data that is inaccurate is erased or rectified without delay. Data subjects have the right to have any inaccurate data corrected at any time.

4.2.5 Storage Limitation

4.2.5.1 Data Retention and Destruction

The school's Data Retention Policy and Schedule must be always adhered to, retaining data for longer than is necessary would constitute a breach of the regulation. Data owners within the school must determine and document processes for ensuring the data retention schedule is adhered to and that data is disposed of accordingly once it reaches the end of its retention period. Processes should include how these practices are monitored.

Confidential and personal data must be securely and permanently deleted or disposed of once the retention requirements have been reached and must be disposed of in a way that protects the rights and privacy of data subjects.

All confidential and personal data is to be shredded and disposed of as 'confidential waste'. Hard drives and portable media must be disposed of securely using approved third parties as necessary.

4.2.6 Integrity and confidentiality – Data Security

4.2.6.1 Access and Storage

The school shall implement appropriate security, technical and organisational measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Example measures to ensure the level of security appropriate to risks of processing personal data include

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Data Processing
- The pseudonymisation and encrypting of data when and where appropriate

Recommended security procedures include:

- **Entry controls.** Awareness within the school to report any stranger seen in entry-controlled areas to a member of the senior management team.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.). It is the individual responsibility of every employee to clear their desk or work area of any confidential information (which includes any information relating to an identifiable individual).
- **Methods of disposal.** Paper documents must be shredded. Digital storage devices must be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the applicable policies.
- **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- **Working away from the school premises – paper documents.** Employees are discouraged from removing paper documents containing confidential information from the school site. However, where this is necessary, measures need to be put in place to ensure the security of the documents. They must not be left in an unattended vehicle, not worked on in public and if taken home they must be secured in a locked cupboard until returned to school.
- **Working away from the school premises – electronic working.** Employees can access the school network securely from a remote device and when doing so the same security precautions must be taken. USB sticks are prohibited unless encrypted and documents must not be downloaded and stored in personal folders if they contain any personal data attributable to an individual student or employee.
- **Document printing.** Documents containing personal data must be collected immediately from printers and not left on photocopiers.
- **Telephone, radio (where applicable) or discussions** in person relating to any confidential matter in respect of an identifiable individual must take place in private and not be overheard.

An employee must only access personal data they need to use as part of their job and where they have been authorised to do so. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

All employees are responsible for ensuring that Confidential and Personal Data held by the school is stored securely against unauthorised or unlawful loss or disclosure.

Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices.

Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

Confidential or personal data must not, under any conditions, be disclosed to any third party, unless that third party has been specifically authorised by the school to receive that information and has entered into a **Data Processing Agreement (DPA)** with the school or has been specifically authorised by the data subject themselves.

Confidential or personal data displayed on computer screens and terminals must not be made visible except to authorised employees and the data subject themselves.

Confidential or personal data must not be removed from the school premises unless necessary and with approval of a Head of School. Personal data will not be transferred outside the UK without appropriate contracts and approval.

4.2.6.2 Anonymisation Requirements

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is likely to take place.

Personal data must be anonymised if it is to be used for a purpose other than which it was collected when consent was obtained (e.g., data analysis, system testing or training).

4.2.7 Accountability

The school takes its accountability very seriously and as such ensures appropriate organizational and technical measures are implemented and reviewed continually.

4.2.7.1 Training

All relevant employees and Governors will undergo training which outlines their responsibilities under this Policy. School employees will undergo this training upon induction and subsequent additional refresher training on a regular basis (annually).

4.2.7.2 Documentation

The school maintains evidential documentation in demonstration of its compliance with the Regulation. This includes Records of Processing, Policies, Processes, Procedures and logs. All documents are subject to a review period and are trained to employees who have access to them, as appropriate, through the school's internal intranet/ shared access folders.

4.2.7.3 Records of Processing

The school will maintain a Record of Processing detailing activity under its responsibility containing the following information,

- The name of the contact details of the school (and where applicable the Joint Controller, the controller's representative and the Data Protection Officer)
- A description of categories of the data subjects and categories of personal data
- Classification and handling of Data
- The lawful basis for processing
- Any 3rd party processing and 3rd country transfers

These records are to be made available to the Information Commissioners Office (ICO) on request.

4.2.7.4 Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 2018 and UK GDPR.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.

4.3 Data Privacy by Design (and default)

The UK GDPR requires the school to integrate data protection concerns into every aspect of our processing activities. This approach is 'data protection by design and by default'. It is a key element

of the GDPR's risk-based approach and its focus on accountability, i.e., our ability to demonstrate how we are complying with its requirements.

4.3.1 Data Protection Impact Assessment (DPIA)

This is a process to help identify and reduce the data privacy risks of a project or a change and should be completed at the outset and throughout the development or implementation of a project / change,

- It enables the school to analyse how a project or a change may affect the privacy of individuals involved systematically
- A DPIA should be applied to new projects to allow greater scope for the project needs to be implemented and should also be used when planning changes to an existing system or BAU process
- The DPIA should ensure privacy risks are minimised whilst allowing the project / change to meet its objectives
- Risks can be identified early in the project / change by analysing how data will be used (risks to data subjects such as potential for damage or distress)
- The DPIA should assess the risks to the school such as the financial and reputational impact of a breach arising from the project (higher risk projects that are likely to be more intrusive are likely to have a higher impact on privacy)

The DPIA process should not need to be overly complex or time consuming, but there is an expectation of a certain level of rigour in proportion to the privacy risks arising from the process or project under review. The school have a documented process and DPIA template which should be used. The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment as well as being part of the final sign off process.

4.4 Data Subject Rights

The school must maintain appropriate procedures to facilitate data subjects exercising their rights and will not refuse to act on such a request unless the school cannot confirm the identity of the data subject.

Data subjects have the rights to:

- Be informed
- Access the information we hold about them (Data Subject Access Request Procedure)
- Have their details rectified if inaccurate
- Have their details deleted if they are not required for lawful reasons
- Object to their data being processed
- Request the processing of their data restricted
- Have automated processing and profiling restricted

- Request information processed by automated means is sent to them (or another nominated Data Controller) in a commonly used electronically readable format

4.4.1 Subject Access Requests (SARs)

The school will provide individuals with a copy of the information held about them within one month of receiving a request. On receiving such a request, the school must check and require evidence to determine the identity of the individual and any further information required to clarify the specifics about the request being made. Where the request is for a child's personal data, any child 13 years or older should either make the request themselves or alternatively, provide consent for a third party (e.g., parent) to seek access.

Where a subject access request has a broad scope, the school may ask for more details from the data subject to locate the specific information that is of interest. Where a large volume of information is held, the school may seek to make the information available in ways other than providing a copy.

The school has (and will maintain) an appropriate Subject Access Request Policy in place that should be referred to in conjunction with this Policy. All Subject Access Requests received will be recorded for monitoring and reporting purposes on the appropriate log.

Requests from individuals to correct, rectify, block, or erase information that they regard as incorrect or to stop processing that is causing damage or distress will be considered by the school on a case-by-case basis. The individual concerned will be fully informed of the resulting decision and the reasons for it.

Data subjects should be able to make SARs and exercise their rights easily and at no cost.

A copy of the schools Subject Access Request form is available on the school website at <https://stjosephshighfield.org/gdpr/> or by contacting info@stjh.bwcet.com

For details of your other rights, please see 'Your Information, Your Rights' booklet on our website at <https://stjosephshighfield.org/gdpr/>

4.5 Data Sharing / Third Party Processing

4.5.1 Sharing with Third Parties

Personal sensitive data will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision (GDPR exemption exists) to allow the sharing of such information.

The school will ensure that supporting processes and documentation are made available so that they understand how to share information safely and lawfully.

Any data sharing with third parties must be done only in agreement with senior leaders and in conjunction with the Headteacher or DPO.

4.5.2 Third Parties

The school may choose to use a third party to provide a service or a product and this may include access to some records. This does not dismiss any responsibility for the safety and security of these records.

Examples of various organisations who may provide services to the school include,

- Payroll provider
- Teachers Pensions
- DBS provider
- Occupational Health
- Recruitment providers
- Education welfare
- Online payment systems
- Student performance progress systems

The school will only choose third parties who provide sufficient guarantees about how they will protect these records and will ensure due diligence is completed along with written and enforceable contracts (Data Processing Agreements/ DPA).

All contractors who are users/processors of personal information supplied by the school will be required to confirm that they will abide by the requirements of the Regulation to the same standard as the school.

All third parties to the school must ensure they, and all their staff who have access to personal data, held or processed for or on behalf of the school, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Regulation. Any breach of any provision of the Regulation will be deemed as being a breach of the contract between the school and that third party. The school shall take reasonable steps to ensure regular monitoring of contracts and specifically the security of data being processed on its behalf and must allow data protection audits by the school if requested, in line with these contractual arrangements.

Any observed or suspected security incidents or security concerns should be reported to the Headteacher or DPO immediately in line with the Data Breach Process.

Third parties will not be able to sub-contract Data Processing without the explicit written permission of the school.

The school may have a duty to disclose personal information to comply with legal or statutory obligation. The DPA 2018 may permit the school to share data without consent or without informing individuals in accordance with the Right to be Informed:

- With the police and law enforcement bodies where it is considered necessary for the prevention and detection of crime;
- Where the information may be necessary under enactment, for the purposes of legal proceedings and or for exercising of defending legal rights; and
- Where the processing is necessary because it is a task carried out for in the public interest, for example, sharing information with the local authority, for example Safeguarding and Child Protection.

CCTV System

The school operate an overt CCTV system across the school site. This includes CCTV cameras which are located externally and internally within the school building. Images captured by the CCTV system are necessary for the prevention and detection of crime, and site security. The school has a CCTV Policy governing the details, the purposes, use and management of the CCTV system, and the school has implemented procedures that must be followed to ensure that the school complies with data protection, human rights and statutory codes of practice published by the Information Commissioner

All personal data captured on the CCTV system will only be processed in accordance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the school/academy will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and the 12 guiding principles contained therein.

4.5.3 Joint Controllers

Where two or more controllers jointly determine the purpose and means of processing, it is referred to as being 'Joint Controllers'. Where this is the case, the school and the other Joint Controller shall in a transparent manner determine their respective responsibilities for compliance with the Data Protection Regulations, with regards to exercising the rights of the data subject and their respective duties to provide the information and gain consent. In these situations, documented contracts are required by way of a Data Sharing Agreement (DSA).

4.6 Data Breaches

All data breaches (however minor) should be reported via the process detailed in the school's Data Breach Process.

The definition of a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A personal data breach may (if not addressed in an appropriate and timely manner) result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Therefore, as soon as anyone within the school becomes aware of a personal data breach this should be considered very seriously and acted upon immediately.

All personal data breaches must be reported in line with the procedure without undue delay (and not later than 72 hours after having become aware of the breach). The school Data Breach Process should be read in conjunction with this Policy.

4.6.1 Complaint Handling Requirements

Processes and procedures are in place and maintained for handling complaints relating to Data Protection. The Headteacher/DPO must be notified of any upheld complaints relating to data protection and must be kept informed of any correspondence with the individual making a complaint.

5 Policy Governance

Monitoring to assess the adherence to and effectiveness of this policy will be completed periodically by the senior leadership team, Headteacher, DPO and School Directors.

Monitoring should be conducted on a regular basis, but no less than once annually. Output for the monitoring should be reported to Headteacher/DPO and School Directors.

5.1. Roles and Responsibilities:

First line of audit

All Employees

- All employees are responsible for compliance with the Data Protection Policy and associated procedures at all times
- Employees should report any potential, actual or perceived data breaches to their line manager who will review and escalate when and where necessary and should follow the data breach process (to report potential / actual breaches)
- Ensure any required remediation for suspected or actual data breaches is resolved in a timely manner
- Complete all relevant Data Protection training and awareness including mandatory sight of relevant policies

Leadership Team

- Leaders are responsible for ensuring adherence to this policy and associated procedures and processes within their areas of accountability
- Ensuring and monitoring that working practices within their areas of responsibility are compliant with all data protection regulations
- Establishing and maintaining documented procedures to ensure that anyone requesting confidential or personal data either in person, electronically or by telephone is appropriately authenticated before disclosing information
- Establishing and maintaining documented procedures to ensure personal data relating to customers is kept accurate and up to date

Second Line of audit

The Headteacher, in conjunction with DPO is responsible for ensuring; -

- School registrations with the ICO are maintained
- Ensuring that School policies, processes, standards & controls are adequately defined and implemented to ensure compliance with all Data Protection Regulations
- Challenge and ensure oversight of first line procedures to ensure compliance with all the requirements of this policy and associated standards and controls
- Providing clarification and guidance on any aspect of compliance with all data protection regulations.

If you observe a breach of this Policy, please speak to your line manager or the Headteacher/DPO immediately.

Any failure to comply with this Policy may constitute a disciplinary matter for the person concerned and, in some cases, they could also incur employment or personal liability (where applicable).

For any clarification, please refer to your Leadership team, the Headteacher or DPO.

6. Definitions

Controller	The school who process Personal Data.
DP Legislation	All relevant data protection legislation, ICO codes of practice and FCA guidance which applies to the school and includes the UK Data Protection Act 2018, the UK General Data Protection Regulation, the Privacy and Electronic Communications Regulations 2003 and the Directive on Privacy and Electronic Communications (the ePrivacy Directive).
Data Subject	An individual who is the subject of any Personal Data.
DPIA	Data Privacy Impact Assessment
Data Protection Officer (DPO)	The individual within the school who has oversight for data protection compliance.

GDPR	The UK General Data Protection Regulations which is a regulation in on data protection and privacy for all individuals within the United Kingdom.
ICO	The Information Commissioner's Office who are the UK regulator that is responsible for the oversight and enforcement of Data Protection legislation.
Personal Data	Data relating to a living individual.
Policy	The Data Protection Policy.