St Joseph's Roman Catholic High School

Information Management Policy

Jesus Christ is our family role model
Opening our hearts and minds to dream the impossible and achieve beyond our wildest imagination
Everybody is valued and respected
Young and old will journey together to build God's Kingdom.
Striving for academic excellence and celebrating success in all we do

Approved by Governors: March 2022	**Review: March 2024**
Date:	**Date:**

Version Control & Amendment History

Version / Issue No.	Date	Author	Remarks / Reason for Change
V.01	15/11/2021	L Withnell	Merging of Information Management Policy and GDPR Policy
V.02	02/10/2023	C Roberts	Staffing Updates

V 0.1	***15.11.21***	***Details of changes made***
Page No	***Points***	**Changes**
	Retention schedules and impact levels	Retention schedule removed on advice from the Policy on the recommendation of the DPO. Please see the Retention schedule Document.
	Training	Training is to be annually rather than just on induction.

Contents Page

1 Statement of Intent

St Joseph's RC High School is required to keep and process certain information about its staff members, students, parents, governors, visitors and other individuals in accordance with its legal obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

The school may, from time to time, be required to share personal information about its staff and students with other organisations, mainly the LA, other schools and educational bodies and potentially Children's Services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative and St Joseph's RC High School believes that it is good practice to keep clear practical policies, backed up by written procedures.

2 Aims

Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK Data Protection Law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3 Legislation and Guidance

This policy meets the requirements of the:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

4 Definitions

TERM	DEFINITION
Personal Data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or Ethnic origin • Political opinions • Religious or Philosophical beliefs • Trade Union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5 The Data Controller

Our school processes personal data relating to parents, students, staff, governors, visitors and others and therefore is a data controller.

The school is registered with and has paid its data protection fee to the ICO, as legally required.

6 Roles and Responsibilities

This policy applies to **all staff** employed by our school and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1 Governing Body

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

6.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governing Body and where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The schools DPO is Mr M Keeffe, contactable through office@st-josephs.bolton.sch.uk.

6.3 Headteacher

The Headteacher acts as the representative of the Data Controller on a day-to-day basis.

6.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

7 Data Protection Principles

The UK GDPR is based on data protection principles that our school must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

8 Collecting Personal Data

8.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life

- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**

- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden

- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent**

- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made **manifestly public** by the individual

- The data needs to be processed for the establishment, exercise or defence of **legal claims**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

8.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

9 Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/guardian that puts the safety of our staff at risk

- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:

    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law

    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with Law Enforcement and Government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

10 Subject Access Requests and Other Rights of Individuals

10.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

10.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.
Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or guardians of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we cannot reasonably anonymise and we do not have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above) and to receive information when we are collecting their data about how we use and process it (see Section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11 Parental Requests to see the Education Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

12 Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system. We will provide alternative means of accessing the relevant services for those students. For example, students can use the Reval machine to credit money to their school dinner account.

Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system, we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

13 CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's Code of Practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr J Butler, Network Manager via office@st-josephs.bolton.sch.uk.

14 Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

15 Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing and always in line with the data protection principles set out in relevant data protection law (see Section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply

- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16 Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept in a secure manner when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access

- Users must not remove or copy sensitive or personal data from the school unless specifically given permission to do so. Media should be encrypted and transported securely for storage in a safe location. When data is required by an authorised user, from outside the school premises, for example, by a teacher working from home, they must have secure remote access to the Management Information System (MIS) or Learning Platform

- Secure remote access to the Management Information System or to the school network can only be obtained using the SOPHOS Authenticator application which can be obtained from the ICT Office

- Secure remote access to the Learning Platform is achieved using RMUnify

- Sensitive or personal information must be securely deleted when no longer required

- Computer passwords should not be disclosed between users

- Files and paperwork that identifies individuals must never be left unattended and must be stored in locked cabinets within a controlled access room which must be locked when not in use

- All staff processing personal information should be appropriately trained

- Passwords used to access school computers, laptops and other electronic devices should be at least 12 characters long and users are encouraged to use complex passwords which contain letters, numbers and symbols. Staff and students are reminded that they should not reuse passwords from other sites.

- Staff are expected to use Microsoft 'One Drive' for the secure transfer of data between home and work.

- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see Section 8)

17 Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with Data Protection Law.

18 Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium

- From February 2022, all data breaches should be reported using the data breach form (see Appendix 2). This form is also available from the DPO Lead and DPO and on Microsoft Teams

- Safeguarding information being made available to an unauthorised person

- The theft of a school laptop containing non-encrypted personal data about students

19 Training

All staff and governors are provided with data protection training as part of their induction process. Data protection training should also been done on an annual basis and will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20 Monitoring Arrangements

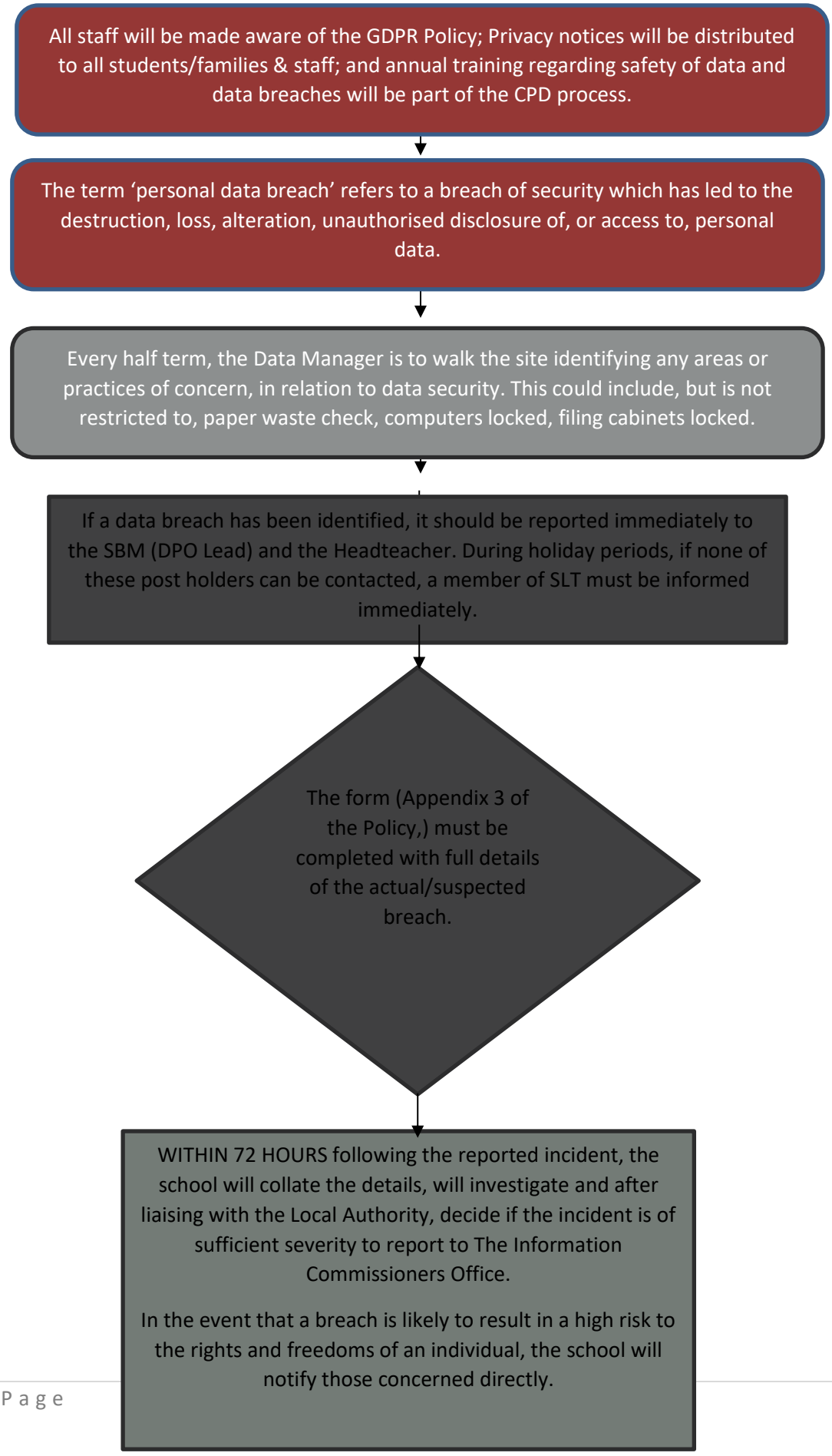
The Data Protection Lead is responsible for monitoring and reviewing this policy. This policy will be reviewed every **2 years** and shared with the Full Governing Body.

21 Links with Other Policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding Policy
- CCTV Policy
- Biometrics Policy
- Data Retention Policy

Appendix 1: Procedures for identifying and reporting of data breaches



Appendix 2: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the Data Protection Officer, Mr M Booth (DPO Lead) or Ms L Withnell (DPO)

- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- Staff and Governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Headteacher and the Chair of Governors

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary and the DPO should take external advice when required

- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences. If appropriate, DPO will liaise with the Headteacher

- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are kept with the Headteacher and a record is made by the DPO on the Data Breach Log

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:

    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach on the Data Breach Log, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible and reported to Governors at their termly meetings
- The DPO and Headteacher will meet when necessary to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to Minimise the Impact of Data Breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Special Category Data

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will liaise with the Headteacher. They will consider whether it is appropriate to contact relevant unauthorised recipients, explain that the information was sent in error and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

General Data Breaches

Include but are not limited to the following:

- Details of student premium interventions for named children being published on the school website
- Non-anonymised student exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 3

Information Security Incident Report Form

All boxes must be completed

To be completed by the person reporting the breach

Name	
Job title	
School	
Telephone number	
E-mail address	
Date	
What has happened? Please provide as much information as you can about what has happened, what went wrong and how; include a description of the data, e.g. format, volume, from which system, and the location of the breach.	
How did you find out about the breach? If you were not the person who originally found there had been a breach, please explain how you found out about it <u>and</u> how they found out about it.	

Was the breach caused by a cyber incident?					
Yes		No		Not yet known	

When was the breach discovered?	Date:		Time:	
When did the breach occur?	Date:		Time:	

What has happened to the information? (Please select all that apply)					
Destroyed		Lost		Stolen	
Altered		Unauthorised Disclosure		Unauthorised Access	
Other *(please give details below)*					

Categories of personal data included in the breach *(Please select all that apply)*			
Basic personal identifiers *(e.g. name, contact details)*		Identification data *(e.g. usernames, passwords)*	
Racial or ethnic origin		Political opinions	
Religious or philosophical beliefs		Trade union membership	
Health or medical data		Sexual life or orientation	
Gender reassignment data		Genetic or biometric data	
Financial information		Criminal convictions or offences	
Official documents *(e.g. driving licenses)*		Location data	
Other (please give details below)		Not yet known	

How many people could be affected?	

Categories of data subjects affected *(Please select all that apply)*			
Students		Staff	
Parents / Carers		Governors	
Volunteers		Other (please give details below)	

What is the possible impact of the breach on the data subjects?

Has there been any actual harm to data subjects? *(If yes, please give details below)*					
Yes		No		Not yet known	

What is the likelihood that data subjects will experience significant consequences because of the breach? (Please select one option and give further details below)					
Very likely		Likely		Neutral	
Unlikely		Very unlikely		Not yet known	

Have you told the data subjects about the breach?

Yes		About to or in process of telling them	
No, but they're already aware		No, but planning to tell them	
No, decided not to tell them		Not yet decided whether to tell them	
Seeking advice from DPO		Other (Please give details below)	

Have you told, or are you planning to tell, any other organisations (e.g. police, regulatory body) about the breach? *(If yes, please give details below. If you have a crime reference number, please include it)*

Yes		No	
Seeking advice from DPO		Other (Please give details below)	

What measures have been taken to deal with the breach? *(e.g. contacting the person sent in formation in error, auto-erased lost laptop)*

Has the data been recovered? (Please give details - if the breach is due to a misdirected email, include whether you have had confirmation that the recipient has deleted it and whether it was read or unread)

Yes		No		Partially	

What measures have been taken / are proposed to mitigate further breaches?

If there is any further information you think should be considered, please include it here.

To be completed by the Data Protection Officer

Form received by DPO	**Date:**		**Time:**			
Was the form received within 24 hours of the breach being discovered?			Yes		No	
If no, was a reason given? (Please give details below)			Yes		No	

Is the information on the form complete?	Yes		No	
If not, what further information is required? *(Please give details below)*				

Breach reported to SIRO	Yes		No		Date	
Breach reported to Head Teacher	Yes		No		Date	
Breach reported to Chair of Governors	Yes		No		Date	

What measures have been agreed should be taken to deal with the breach?
What measures have been agreed should be taken to mitigate harm caused by the breach?

Have data subjects been told about the about the breach (if not already done by person reporting it)?			
Yes		About to or in process of telling them	
No, but they're already aware		No, but planning to tell them	
No, decided not to tell them		Other (Please give details below)	

Does the breach warrant a report to the ICO?	Yes		No	
If yes, when was the breach reported to the ICO?	Date:		Time:	
Was report to ICO made within 72 hours?	Yes		No	

If report was not made within 72 hours, please provide justification for late reporting below.
What has been identified as the root cause(s) of the breach following investigation?
What corrective actions have been identified following investigation?

Action	Target Date	Owner	Date Completed

DPO Sign-off		**Date**	
Head Teacher Sign-off		**Date**	
Date Incident Investigation Closed			