St Joseph's Catholic Primary School

Inspiring everyone to **REACH** through Faith, Hope, Love

At St Joseph's, we strive for academic excellence through encouraging resilience, empathy, aspiration and challenge. We have high expectations for ALL so that we can be 'The best we can be.' With Faith, Hope and Love at the heart of our school family, our children feel safe, secure and supported.

Data Protection Policy

Including the Protection of Biometric Information of children

Reviewed by:	Charlotte Claridge
Approved by FGB:	18th May 2022
Review Cycle:	Annually
Review due:	May 2023
Other relevant policies:	Safeguarding & Child Protection, Acceptable Use of ICT, e-Safety, FOIA Publication Scheme, Privacy Notices

Approval History

Version no	Approve by	Approval date	Comments
V1.0	FGB	18/05/2022	New Policy 2022

Document Author/Owner

Version	Authors	Role
V1.0	Charlotte Claridge	Data Protection Officer/Manager

Document Governance

Next Review Date	May 2023 Department for Education's recommendation in its advice on statutory policies. Annual audit
Circulation	This framework is to be made available to all employees of St Josephs Catholic Primary School
Information Classification	NOT PROTECTED

Contents

1. Aims

St Joseph's Catholic Primary School is committed to managing confidential information in accordance with the requirements of the General Protection Regulation and Data Protection Act 2018. Our school aims to ensure that all personal data collected about staff, pupils, 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.

2. 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)

3. 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.

TERM	DEFINITION
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.

4. The data controller

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

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

5. 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.

5.1 Governing board

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

5.2 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 board 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.

Our DPO is our SBM and is contactable via 01453 860311

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 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

6. 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.

7. Collecting personal data

7.1 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 pupil) 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 pupil) 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 pupil) 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.

7.2 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.

8. 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 pupil or parent/carer 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 pupils – 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 that affects any of our pupils or staff.

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

9. Subject access requests and other rights of individuals

9.1 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 isn't 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. Direct the party to the St Joseph's website and complete appendix 1 for our subject access request form.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer 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 below the age of 12 are generally not 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 carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 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 pupil 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 can't reasonably anonymise, and we don't 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 consider 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.

9.4 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 and have **Right to be forgotten**

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped, and that all their personal data is erased by the school including any data held by contracted processors.

It should be noted that for photographs/videos published on a Social Media site retrospective deletion of the photograph/video may not be possible if it has been shared by a third party.

- 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.

10. Parental requests to see the educational 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 pupil) 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 pupil 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 pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Data protection impact assessments (DPIA's)

Prior to processing data, including biometric data, or implementing a system that involves processing data or biometric data, a DPIA will be carried out.

The DPO will oversee or monitor the process of carrying out the DPIA.

The DPIA will:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the data, including biometric data begins.

The ICO will provide the school with a written response (within 8 weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, he ICO may advise the schools not to carry out the processing.

12. Biometric recognition systems

At St Josephs we do not currently use biometric systems, however for when we do, we have included the below definitions and processes:

(i) Definitions

Biometric Data: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including the use of fingerprints, facial shape, retina and iris patterns, and hand measurements.

Automated biometric recognition systems: A system which measures and individual's physical or behavioural characteristics by using equipment that operates "automatically" (i.e. electronically). Information from the individual s automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

Processing biometric data: Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes date when:

- Recording pupils' biometric data, e.g. taking measurements from fingerprints via a fingerprint scanner.
- Storing pupils' biometric information on a database.
- Using pupil's biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, it is considered special category data.

(ii) Protection Principles in relation to Biometric information

St Joseph's Catholic Primary School will process all personal data, including biometric data in accordance with the key principles set out in the GDPR and will ensure that all biometric data is:

- Processed lawfully, fairly and in a transparent manner
- Only collected for specific, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
- Accurate and, where necessary, kept up to date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to sign in 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 pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can sign in through name registration.

Parents/carers and pupils 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 pupil 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 pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), 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. 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 for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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 pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

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

- Within school on notice boards and in school newsletter, promotional material 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 e-safety and acceptable use of ICT policy for more information on our use of photographs and videos.

14. 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, and 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

15. 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 under lock and key 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils 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)

Please see appendix 2 for our information security procedures.

16. 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.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

Please see appendix 3 for our records management procedure.

17. Personal data breaches

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

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 4.

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 pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff, volunteers, and governors are provided with data protection training as part of their induction process and on-going training will take place as necessary through inset and staff meetings and all training is logged in our master training spreadsheet to ensure all have the necessary support to ensure they follow the expected practice. Found on the **Gdrive-winword-SBM-Training**

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy, complimented with completing data audits and training annually.

The headteacher is responsible for ensuring provision in this policy is implemented consistently.

This policy will be reviewed annually and approved by the full governing board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E-safety
- Acceptable use of ICT
- Privacy notices

Appendix 1: SUBJECT ACCESS REQUEST FORM

You should complete this form if you want us to supply you with a copy of any personal data we hold about you. You are currently entitled to receive this information under the Data Protection Act 1998 (DPA) and will continue to be under the EU General Data Protection Regulation(GDPR),which came into effect on 25 May 2018. We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavor to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or

- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.
You are not obliged to complete this form to make a request but doing so will make it easier for us to process your request quickly.

SECTION 1: Details of the person requesting information

Full name:	
Address:	
Contact telephone number:	
Email Address:	

SECTION 2: Are you the data subject?
Please tick the appropriate box and read the instructions which follow it.

Yes: I am the data subject. I enclose proof of my identity (see below). (Please go to section 4)

No: I am acting on behalf of the data subject. I have enclosed the data
Subject's written authority and proof of the data subject's identity and my own identity (see below). (Please go to section 3)

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) Proof of Identity

Passport, photo driving licence, national identity card, birth certificate

2) Proof of Address

Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 3: Details of the data subject (if different from section 1).

Full name:	
Address:	
Contact telephone number:	
Email address:	

SECTION 4: What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

Please note if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of other, we may not be able to disclose the information to you. In which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with section 8(2) of the DPA, not to provide you with copies if information requested if to do so would take 'disproportionate effort', or in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be 'manifestly unfounded or excessive'. However we will make every effort to provide you with satisfactory form of access or summary of information suitable.

SECTION 5: Information about the collection and processing of data.

If you want information about any of the following, please tick the boxes:

- Why we are processing your personal data
- To whom your personal data are disclosed
- The source of your personal data

SECTION 6: Declaration.

Please note that any attempt to mislead may result in prosecution.

Information that I have read and understood the terms of this subject access form and certify that the information given in this application is true. I understand that it is necessary for St Joseph's Catholic Primary School to confirm my/ the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed…….. **Date**……

Appendix 2: INFORMATION SECURITY PROCEDURE

Type	Example	Security implementation	Management
Technical	Data Corruption Malware Corrupt Code Hacking	https encryption technology firewalls Password protection	Edit IT/ DPO
Physical	Unescorted visitors in secure areas Break-ins to centres Thefts from secure centres Theft from unsecured vehicles/centres Loss in transit/post	Visitor policy procedure Burglar alarm Off-site storage procedure Confidentiality agreement Data breach procedure	Safeguarding procedures / Visitor procedures Privacy notice
Human Resources	Data Input errors Non-secure disposal of hardware or paperwork Unauthorised disclosures Inappropriate sharing- Inappropriate lockdown of systems	Annual audit procedure Records management procedure Data breach reporting procedure Privacy control- section 7	DPO/Head to oversee

Appendix 3: RECORDS MANAGEMENT

Type of Record	Trigger	Minimum Retention period at School	Final Action
Accident Records(children)	Date of incident	25 Years	Destroy
Accident/injury at work records (staff)	Date of incident	12 years	Review
Accounting records (other than annual accounts)	End of the financial year	6 years	Destroy
Accounts (Annual)	End of financial year	6 years	Archive – In-house
Administrative files (routine)	End of administrative use	5 years	Review to see whether a further retention period is required
Admission registers	Date of last entry	6 years	Archive – In-house
Attendance registers	End of academic year	3 years	Destroy
Biometric Information	End of administrative use	Immediate	Destroy
Contracts under seal	End of contract	12 years	Destroy
Contracts under hand	End of contract	6 years	Destroy
Contract monitoring records	End of current year	2 years	Destroy
Data Images		Indefinitely.	
Development plans (school)	End of administrative use	6 years	Archive – In-house/Diocese
Free School Meal Registers	End of current year	6 years	Destroy
Governors' reports	Date of meeting	6 years	Archive – Sharepoint/ In-house
Instruments of Government		Retain permanently until closure of school	Archives – deposit at Gloucestershire Archives
Maintenance logs	Date of last entry	10 years	Destroy
Minutes of governors, staff and PTA meetings	End of academic year	6 years	Archives – Sharepoint/ In-house
OFSTED reports and papers	Superseded by new report	Review on replacement by	Archives – In-house

		new inspection report	
Policies	Superseded by new policy	Retain in schools whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Archives – In -house
Property title deeds and architects plans	No longer used regularly	Permanent	Archives – Diocese
Pupil files and record cards (primary)	Pupil leaves school	Immediate	Transfer records to secondary (or other primary) school
SAT's/PAN/Value added records	End of academic year	6 years	Destroy
School Prospectus	End of academic year	3 years	Archives – In-house
Scrap books and photograph albums	End of administrative use	Immediate	Archives – In-house
Special Educational Needs (SEN) Files	Date of last entry in file	30 years then review	Destroy unless legal action pending. Some LA choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education "case.
Special Educational Needs and Disability Act 2001 Section 1: statements	Date of Birth	30 years	Destroy unless legal action pending
Staff – personnel files	End of employment	12 years	Destroy

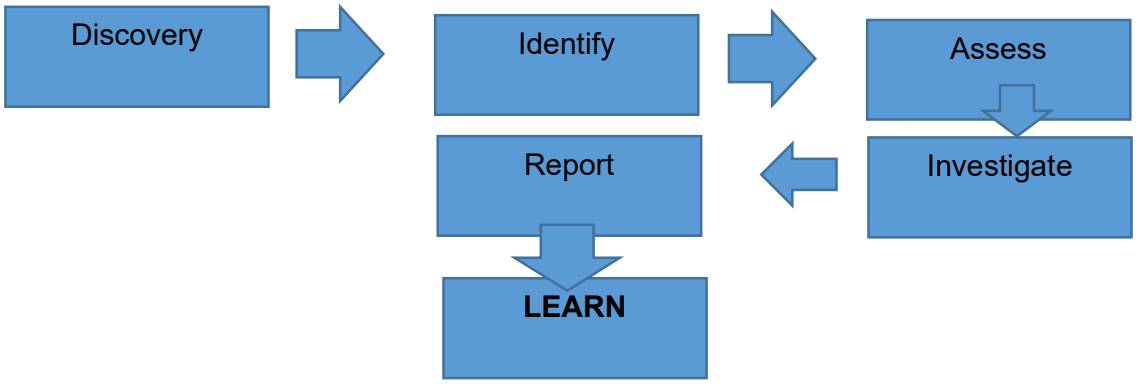
Appendix 4: PERSONAL DATA BREACH PROCEDURE

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 (DPO).
- The DPO will investigate through the below process:

Outline Process for incidents

Diagram below shows the flow of actions involved in a Personal Identifiable Information Breach Investigation



Discovery/Identify/Assess/Investigate - Breaches and weaknesses need to be reported at the earliest possible stage to the data protection officer on the form below:

DATA PROTECTION BREACH REPORTING FORM

The aim of this document is to ensure that in the event of a security incident such as data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk to the school/students/employees/parents/careers.

The checklist can be completed by anyone with knowledge of the incident. It will also require review by the Data Protection Officer who can determine Data Protection Act implications and assess whether changes are required to existing business processes.

1. Summary of Incident	
Date and Time of Incident	
Number of people whose data is affected	

Department/ Class effected	
Nature of breach e.g. theft/disclosed in error/technical problems	
Description of how breach occurred	
2. Reporting	
When was breach reported?	
How you became aware of the breach:	
Has the data Protection Officer been informed.	
3. Personal Data	
Full description of personal data involved (without identifiers);	
Number of individuals affected:	
Have all affected individuals been informed:	
If not, state why not:	
Is there any evidence to date that the personal data involved in this incident	

has been inappropriately processed or further disclosed? If so, please provide details:	
4. Data Retrieval	
What immediate remedial action was taken:	
Has the data been retrieved or deleted? If yes - date and time:	
5. Impact	
Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? If so, provide details:	
6. Management	
Do you consider the employee(s) involved has breached information governances policies and procedures:	

Please inform of any disciplinary action taken in relation to the employee(s) involved:	
Had the employee(s) completed data protection training:	
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this:	
Has there been any media coverage of the incident? If so, please provide details	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure:	

- Once the above has been reviewed decide 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 (e.g. from IT providers).
- 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
- 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 stored; **Gdrive-winword-SBM-GDPR-DB**
- 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, 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)

  Records of all breaches will be stored: **Gdrive-winword-SBM-GDPR-DB**
- 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
- The DPO and headteacher will meet termly 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.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- 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 the external recipients and remove it from the school's email system only retaining a copy if required as evidence.
- In any cases where the recall is unsuccessful the DPO will consider whether to contact the relevant unauthorised individuals who received the email, 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 comprised, the DPO will inform the DSL and discuss whether the school should inform any, or all, of its local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil 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 5: LOG OF REPORT

Incident	Data	Personal Data	Data Retrieval	Impact	Management

Appendix 6: AUDIT LOG

Audit- Who/What	When- Date	Why- Reason	Conclusion	Learning	Next steps