Growing and Achieving Excellence, Inspired by Faith

St Joseph's Catholic Primary School

Data Protection Policy

Approved:	**Autumn 2024**
Review Date:	**Autumn 2025**
Signed: (Headteacher)	**Lorraine Flower**
Signed: (Chair of Governors)	**Andy Waterworth**

Contents:

Statement of intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. Sharing data without consent
9. The right to be informed
10. The right of access
11. The right to rectification
12. The right to erasure
13. The right to restrict processing
14. The right to data portability
15. The right to object
16. Automated decision making and profiling
17. Privacy by design and privacy impact assessments
18. Data breaches
19. Data security
20. Publication of information
21. Photography
22. Data retention
23. DBS data

Statement of intent

St Joseph's Catholic Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK GDPR.

The school may, from time to time, be required to share personal information about its staff or pupils 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 UK GDPR.

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

1. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Act 2018

This policy also has regard to the following guidance:

1. ICO (2018) 'Guide to the General Data Protection Regulation (UK GDPR)'
2. DfE (2018) 'Data protection: a toolkit for schools'

This policy will be implemented in conjunction with the following other school policies:

1. Freedom of Information Policy
2. Safeguarding Policy
3. Acceptable Use Policies
4. Online Safety Policy

2. Applicable data

a. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

b. **Sensitive personal data** is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those that were in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

a. In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

b. The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

4. Accountability

a. St Joseph’s Catholic Primary School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

b. The school will provide comprehensive, clear and transparent privacy policies.

c. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

d. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

e. The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

f. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

a. A DPO was appointed in order to:

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

b. Gary Hipple schoolsdpo@richmondandwandsworth.gov.uk was appointed to the role of DPO.

c. The individual appointed as DPO has the professional experience and knowledge of data protection law, particularly that in relation to schools.

6. Lawful processing

a. The legal basis for processing data will be identified and documented prior to data being processed.

b. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:

— Compliance with a legal obligation.
— The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
— For the performance of a contract with the data subject or to take steps to enter into a contract.
— Protecting the vital interests of a data subject or another person.
— For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

c. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:

— Carrying out obligations under employment, social security or social protection law, or a collective agreement.

- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

d. Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school ensures that the requirements outlined in 7g and 7h are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

7. Consent

a. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

b. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

c. Where consent is given, a record will be kept documenting how and when consent was given.

d. The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

e. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

f. Consent can be withdrawn by the individual at any time.

g. Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in 7b, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

h. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined in 7.2.

8. Sharing data without consent

a. The school may share information without consent in specific circumstances. To determine whether information can be shared with consent, the school will identify one of the other lawful bases for processing:

- **Contract** – the processing is necessary for a contract held between the school and individual, or because the individual has asked the school to take specific tests before entering into a contract.
- **Legal obligation** – the processing is necessary for the school to comply with the law (not including contractual obligations).
- **Vital interests** – the processing is necessary to protect someone's life.
- **Public task** – the processing is necessary for the school to perform a task in the public interest or for it's official functions, and the task or function has a clear basis in law.
- **Legitimate interests** – the processing is necessary for the school's legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests.

b. Where the school is able to justify one of the lawful bases outlined in 8.1, an exemption applies, or there is a requirement under another law, information may be shared without consent.

c. Specifically, the UK GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

9. The right to be informed

a. Adults and children have the same right to be informed about how the school uses their data.

b. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

c. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:

— Withdraw consent at any time.
— Lodge a complaint with a supervisory authority.

- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

d. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

e. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school

holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

f. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

g. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. The right of access

a. Individuals, including children, have the right to obtain confirmation that their data is being processed.

b. Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

c. The school will verify the identity of the person making the request before any information is supplied.

d. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

e. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

f. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

g. All fees will be based on the administrative cost of providing the information.

h. All requests will be responded to without delay and at the latest, within one month of receipt.

i. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

j. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

k. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

11. The right to rectification

a. Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

b. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

c. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

d. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

e. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

a. Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

b. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed

- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

c. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

d. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

e. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

f. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

a. Individuals, including children, have the right to block or suppress the school's processing of personal data.

b. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

c. The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data

- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

d. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

e. The school will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

a. Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.

b. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

c. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

d. Personal data will be provided in a structured, commonly used and machine-readable form.

e. The school will provide the information free of charge.

f. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

g. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

h. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

i. The school will respond to any requests for portability within one month.

j. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

k. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

a. The school will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

b. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

c. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

d. Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

e. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

f. Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

16. Automated decision making and profiling

a. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

b. The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

c. When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

d. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments

a. The school will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

b. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

c. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

d. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

e. A DPIA will be used for more than one project, where necessary.

f. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

g. The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

h. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

18. Data breaches (Appendix 1)

a. The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

b. The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

c. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

d. All notifiable breaches will be reported to the school DPO within 72 hours of the school becoming aware of it.

e. The risk of the breach having a detrimental effect on the individual, and the need to notify the school DPO, will be assessed on a case-by-case basis.

f. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

g. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the school DPO.

h. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

i. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the school DPO or the public need to be notified.

j. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

k. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

a. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

b. Confidential paper records will not be left unattended or in clear view anywhere with general access.

c. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

d. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

e. Memory sticks **will not** be used to hold school data.

f. All electronic devices are password-protected to protect the information on the device in case of theft.

g. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

h. Staff and governors will not use their personal devices (laptops/computers/tablets/phones) for school purposes.

i. Outside of the school, staff will access the school data via SJPK Remote Access Server supported by LGFL Fredom2Roam or via Google Apps.

j. Google files sharing with outside of the school organisation recipients is always done via Copy Link function.

k. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

l. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

m. Circular emails to parents are sent primarily via ParentMail and occasionally via email blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

n. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

o. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

1.1. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

1.2. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

1.3. St Joseph's Catholic Primary School takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

1.4. The Headteacher is responsible for continuity and recovery measures are in place to ensure the security of protected data.

2. Publication of information

2.1. St Joseph's Catholic Primary School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

2.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

2.3. St Joseph's Catholic Primary School will not publish any personal information, including photos, on its website without the permission of the affected individual.

2.4. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

3. Photography

3.1. The school understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

3.2. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

3.3. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

3.4. Precautions are taken when publishing photographs of pupils, in print, video or on the school website.

3.5. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

4. Data retention

4.1. Data will not be kept for longer than is necessary.

4.2. Unrequired data will be deleted as soon as practicable.

4.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

4.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

5. DBS data

5.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

5.2. Data provided by the DBS will never be duplicated.

5.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Appendix 1 Data Breach Procedure

Policy Statement

St Joseph's Catholic Primary School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by St Joseph's Catholic Primary School and all school staff, Governors, volunteers and contractors, referred to hereinafter as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at St Joseph's Catholic Primary School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the School's Data Protection Officer (DPO) or the nominated representative School Business Manager (SBM). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The DPO or the SBM must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. the DPO or the SBM must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The DPO or the SBM must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

5. The DPO or the SBM must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. The use of back-ups to restore lost/damaged/stolen data.

c. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

d. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the DPO or the SBM to fully investigate the breach. The DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and

recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO or the SBM should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the DPO or the SBM should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The DPO and the SBM should ensure that staff are aware of the School’s Data Protection Policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School’s Data Protection Policy and associated procedures, they should discuss this with the DPO or the SBM.

Growing and Achieving Excellence, Inspired by Faith

Data Breach Reporting Form

Please complete the form below to notify the Data Protection Officer of a data protection breach, Please email to Gary Hipple ghipple@wandsworth.gov.uk

	Report prepared by: **Date:** **On behalf of:**	*St Josephs Catholic primary School*
1	**Summary of the event and circumstances:**	
2	**Type and amount of data (personal/staff, student, parental/carer):**	
3	**Actions taken to retrieve the information and minimise the effect of the breach:**	
4	**Details of notification to affected data subject:** (if applicable) **Has a complaint been received from the affected data subject?**	
5	**Breach of procedure / policy by staff member:**	
6	**Details of Data Protection training provided/taken:**	
7	**Any procedure changes required to reduce risks of future data loss:**	
8	**Conclusion:**	