Autumn | 26-27

# St Joseph's Catholic Primary School

## *Data Breach Policy*

| | |
|---|---|
| **Date ratified by Governors:** | Autumn 2026-27 |
| **Date of next review of the policy:** | Autumn 2027-28 |
| **This policy is reviewed:** | **1 Year** |

**Learn together and grow in God's love**

**Aspiration - Compassion - Community - Faith - Respect – Responsibility**

St Joseph's Catholic Primary School
Commerell Street
East Greenwich
London SE10 9AN

# Table of Contents

Section 1: Introduction ..... 3
Section 2: Definitions ..... 3
Section 3: Roles and responsibilities ..... 3
Section 4: What is a personal data breach? ..... 3
Section 5: Reporting a breach ..... 4
Section 6: Managing the breach ..... 4
Section 7: Assessing the risk ..... 4
Section 8: Notifying the ICO ..... 5
Section 9: Notifying the people affected ..... 5
Section 10: Notifying others ..... 5
Section 11: Recording breaches ..... 6
Section 12: Learning from breaches ..... 6
Section 13: Monitoring and review ..... 6
Appendix 1: Data breach report form ..... 7

## Section 1: Introduction

Data protection law requires the school to keep personal data secure and to act quickly when something goes wrong. This policy explains what a personal data breach is, how staff must report one, and how the school manages, records and learns from breaches.

This policy applies to all staff, governors, volunteers and contractors, and to data processors who handle personal data on the school's behalf. Data processors, such as software suppliers and the CCTV maintenance company, must tell the school about any breach affecting school data without undue delay, as required by their contract.

The school wants staff to report breaches. Mistakes happen, and reporting them quickly is the most important thing anyone can do to limit the harm. Staff who report a breach promptly and honestly will be supported. Deliberately hiding a breach, or a deliberate or reckless breach of data protection rules, may be dealt with under the Staff Disciplinary Policy.

This policy should be read with the Data Protection Policy. It does not form part of any employee's contract of employment.

## Section 2: Definitions

| Term | Definition |
|---|---|
| Personal data | Any information relating to an identified or identifiable living person, including facts and opinions about them |
| Special category data | Personal data needing extra protection, including health, ethnicity, religious beliefs, biometric data and sexual orientation. Safeguarding and criminal offence information also needs extra care |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data |
| Data subject | The person the personal data is about |
| ICO | The Information Commissioner's Office, the UK regulator for data protection |

## Section 3: Roles and responsibilities

| Role | Responsibilities |
|---|---|
| Headteacher (Suzanne Long) | Has overall responsibility for managing breaches; is the first point of contact for reporting a breach; decides, with the DPO, whether to notify the ICO and the people affected |
| In the Headteacher's absence | Judith Harvey |
| Data Protection Officer: Judicium Consulting Limited, lead contact Craig Stilwell (dataservices@judicium.com, 0345 548 7000 option 1) | Advises on assessing, containing and reporting breaches; advises on notifying the ICO and the people affected |
| Senior Administration Officer | Keeps the data breach register |
| All staff, governors and volunteers | Report any breach or suspected breach straight away; help with the investigation; do not try to investigate or notify anyone themselves |

## Section 4: What is a personal data breach?

A breach is about more than data being stolen. It includes any accidental loss, sharing or destruction of personal data. Common examples in schools include:

- sending an email, letter, text message or report to the wrong person, or copying in the wrong recipients
- losing a laptop, memory stick, mobile phone, paper file or register
- leaving confidential papers where others can see them, or putting them in normal waste
- someone accessing a system or records they should not have access to
- entering personal data into an AI tool that the school has not approved
- falling for a phishing email that gives someone access to school systems
- a cyber attack, such as ransomware, that locks or exposes school data
- personal data being lost or damaged by fire, flood or equipment failure
- publishing personal data on the school website or social media by mistake

## Section 5: Reporting a breach

If you know or suspect that a breach has happened, act straight away, even if you are not sure:

1. **Tell the Headteacher immediately**, in person, by phone or by email to slong@stjosephs.greenwich.sch.uk. If the Headteacher is not available, tell Judith Harvey.
2. **Take any simple, immediate step to stop the breach getting worse**, for example recalling an email, asking a recipient not to open an attachment, or retrieving lost papers.
3. **Complete the data breach report form** in Appendix 1 the same day, and email it to the Headteacher.
4. **Do not delete anything** that might be needed as evidence, and do not try to investigate further.
5. **Do not contact the people affected, the ICO or anyone else** about the breach, unless the Headteacher asks you to.

If you are unsure whether something is a breach, report it anyway. The Headteacher and the DPO will decide.

Time matters. The school has only 72 hours from becoming aware of a breach to report it to the ICO where this is required, and the clock may start as soon as any member of staff knows about it.

## Section 6: Managing the breach

When a breach is reported, the Headteacher contacts the DPO and, together, they take immediate steps to:

- confirm whether a breach has happened
- contain the breach and, as far as possible, recover, correct or delete the data that has been lost, damaged or disclosed
- assess the risk to the people affected (Section 7)
- decide whether to notify the ICO (Section 8) and the people affected (Section 9)
- decide whether to notify anyone else (Section 10)
- record the breach in the data breach register (Section 11)

**Emails sent in error.** The sender tries to recall the email straight away. If this does not work, the school asks its IT support provider, ATS, to help. The school contacts the people who received it, asks them to delete it without sharing it, and asks them to confirm in writing that they have done so. Where sensitive information may have been published online, the school asks the website or platform to remove it.

**Lost or stolen devices.** The school asks its IT support provider to change passwords and, where possible, lock or wipe the device remotely. Thefts are reported to the police.

**Cyber attacks.** The school contacts its IT support provider immediately, follows the cyber incident response plan in Section 8 of the Cyber Security Policy, and reports the attack to the police through Action Fraud and, where relevant, to its insurer.

## Section 7: Assessing the risk

The Headteacher and the DPO consider:

- what type of data is involved, and how sensitive it is, for example safeguarding, health or SEND information
- how much data is involved, and how many people are affected
- who the people affected are, especially if they are children
- what has happened to the data, and who now has it
- whether the data was protected, for example by encryption or a password
- what harm could result, such as distress, discrimination, financial loss, identity theft, damage to reputation, or risk to someone's physical safety
- whether the risk has been reduced by the steps already taken

## Section 8: Notifying the ICO

The school must notify the ICO where a breach is likely to result in a risk to people's rights and freedoms. The Headteacher, with advice from the DPO, will report the breach without undue delay and, where possible, within 72 hours of the school becoming aware of it, using the ICO's online breach reporting service or by phoning 0303 123 1113.

The report will include, as far as is known:

- what happened, including the types and approximate number of people and records involved
- the DPO's name and contact details
- the likely consequences of the breach
- what the school has done, or will do, to deal with the breach and reduce any harm

If not all the information is available within 72 hours, the school will report what it knows and send the rest as soon as possible. If a report is made after 72 hours, the reasons for the delay will be recorded.

Where the school decides that a breach does not need to be reported to the ICO, it records why.

## Section 9: Notifying the people affected

Where a breach is likely to result in a high risk to people's rights and freedoms, the Headteacher will tell the people affected without undue delay. Where the people affected are pupils, the school will normally tell their parents or carers. The school will explain, in clear and plain language:

- what has happened
- the likely consequences
- what the school has done, or will do, to deal with it
- any steps they can take to protect themselves
- how to contact the DPO

If contacting people individually would involve disproportionate effort, the school may use another method, such as a message to all parents.

## Section 10: Notifying others

The school will consider whether anyone else needs to be told, for example:

- the police, if there has been a theft or a crime
- the school's insurer
- the Royal Borough of Greenwich or the Diocese
- children's social care or the DSL, if safeguarding information has been disclosed

- banks or other organisations that can help reduce harm
- other organisations whose data is also affected

## Section 11: Recording breaches

Every breach is recorded in the school's data breach register, whether or not it is reported to the ICO. The register is kept by the Senior Administration Officer in a secure, confidential file. For each breach it records:

- the facts and cause of the breach
- its effects and the people affected
- the decisions made about notifying the ICO and the people affected, with reasons
- the action taken to contain it and to stop it happening again

## Section 12: Learning from breaches

After each breach, the Headteacher and the DPO review what happened and agree any changes needed, such as new procedures, extra security or staff training. The Headteacher reviews the breach register with the DPO at least once a year to look for patterns, and reports a summary to the Governing Body.

Staff are encouraged to raise any data security concern with the Headteacher or the DPO, even if nothing has gone wrong yet.

## Section 13: Monitoring and review

This policy is reviewed every year by the Headteacher, with advice from the DPO, and approved by the Governing Body.

## Appendix 1: Data breach report form

Complete this form on the same day and email it to the Headteacher (slong@stjosephs.greenwich.sch.uk). If you do not know an answer, say so. Do not delay sending the form.

| Question | Answer |
|---|---|
| Your name and role | |
| Date and time you completed this form | |
| Date and time the breach happened (if known) | |
| Date and time you found out about it | |
| What happened? | |
| What personal data is involved? (for example names, contact details, safeguarding, health or SEND information) | |
| Whose data is it, and roughly how many people are affected? | |
| Was the data protected, for example by encryption or a password? | |
| Who has, or may have, seen or received the data? | |
| What have you already done to stop it or limit the harm? | |
| Is anyone else aware of the breach (for example the person affected or a recipient)? | |

**For school use only**

| Detail | Information |
|---|---|
| Date and time received by the Headteacher | |
| Date and time the DPO was contacted | |
| Breach confirmed? | |
| Reported to the ICO? If so, date, time and reference. If not, reason | |
| People affected told? If so, date and how. If not, reason | |
| Actions taken to stop it happening again | |
| Entered in the breach register (date and initials) | |