



# St Jude's Church of England Primary School Data Breach Policy and Response Procedure

*Our children  
Our St Jude's Family  
Happy – Inspired – Loved  
The sky is not the limit  
Ready for today - prepared for tomorrow*

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

## **Definitions**

### **Personal Data**

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

### **Special Category Data**

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

### **Personal Data Breach**

*St Jude's Church of England Primary School Data Breach and Response Procedure agreed by governors Dec 2022*

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

### **Data Subject**

Person to whom the personal data relates.

### **ICO**

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

### **Responsibility**

The Acting Headteacher, Claire Douch, has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below:

Data Protection Officer: Elaine Efrat

Email: elaine@ascentassets.com

### **Data Breach Procedure**

#### **What Is A Personal Data Breach?**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive):

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

#### **When Does It Need To Be Reported?**

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes:

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

### **Reporting a Data Breach**

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should follow the **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 Acting Headteacher via email.

Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Claire Douch or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Acting Headteacher will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

### **Managing and Recording the Breach**

On being notified of a suspected personal data breach, the Acting Headteacher will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. To decide, they 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 Acting Headteacher will alert the chair of governors

The School will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).

The School 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 School will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#).

The School 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 on the school's computer system.

### **Notifying the ICO**

Where the ICO must be notified, the School 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 School 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 School 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 School expects to have further information. The School will submit the remaining information as soon as possible.

### **Notifying Data Subjects**

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Acting Headteacher will notify the affected individuals without undue delay.

Where the school is required to communicate with individuals whose personal data has been breached, the Acting Headteacher 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

When determining whether it is necessary to notify individuals directly of the breach, the Acting Headteacher will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the Acting Headteacher will consider alternative means to make those affected aware (for example by making a statement on the School website).

## **Notifying Other Authorities**

The School will need to consider whether other parties need to be notified of the breach. For example:

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

## **Assessing the Breach**

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

## **Preventing Future Breaches**

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;

- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether its necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

The School 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 on the school's computer system.

The DPO and Acting 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 Acting Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

### **Reporting Data Protection Concerns**

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the Acting Headteacher or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

### **Monitoring**

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

### **Links with other policies**

This data protection policy is linked to our:

- Online safety policy
- Safeguarding Policy
- Data Protection Policy

## Policy History

Date Reviewed by governors	15 <sup>th</sup> December 2022
Next Review	15 <sup>th</sup> December 2024

This policy has been agreed by the governing body of St Jude's School and supersedes all previous policies relating to this area.

Chair of Governors: Geraldine O'Brien

Signed:

Date:

***Signed copy in school.***