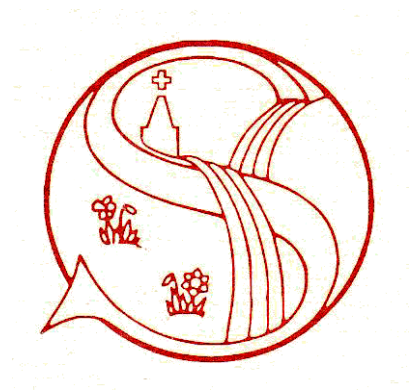


# SPRINGHILL CATHOLIC PRIMARY SCHOOL

*Together we will do our best for Jesus*



## DATA BREACH POLICY

**This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment**

Review: February 2023  
Next review: February 2024

## Introduction

Springhill Catholic Primary School issues this policy to meet the requirements incumbent upon them under the Data Protection Act 2018 for the handling of personal data in its role as a data controller, such personal data is a valuable asset and needs to be suitably protected.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidentally) to avoid a data protection breach that could compromise security.

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

## Scope

This policy applies to all employees of Springhill Catholic Primary School, including contract, agency and temporary staff, volunteers and employees of partner organisations working for Springhill Catholic Primary School.

## Data Breaches

For the purposes of this policy data breaches will include both 'near misses' and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (*e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge*)
- Equipment failure (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data)
- Unauthorised use of, access to, or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data (*e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address*)
- Hacking attack
- Unforeseen circumstances (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data) such as a fire or flood
- Human error
- Breaches of policy such as
  - Server Room door left open
  - Filing cabinets left unlocked
  - Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored (*e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge*)

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

## Risk Assessment and Reporting

The quick response to a suspected or actual data breach is key. When a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, appropriate steps should be promptly taken to address it.

The focus of risk regarding breach reporting is on the potential negative consequences for individuals. On becoming aware of a breach, you should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

All parties in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours, this should be reported as soon as practically possible to the person responsible for the management of personal data breaches within the organisation. This should be done through the completion of the reporting form in [Appendix 1](#), which should be sent to The Headteacher and School Business Manager who will liaise with its Data Protection Officer (One West).

One West can be contacted by email on [i-west@bathnes.gov.uk](mailto:i-west@bathnes.gov.uk) or telephone on 01225 395959

Notify the ICO (if necessary) the personal data breach is likely to result in a risk to the rights and freedoms of an individual(s), the incident may need to be reported to the Information Commissioner's Office (ICO), no later than 72 hours after becoming aware of the breach. It is therefore crucial that you report any data breach (regardless of the severity) to your Data Protection Officer (DPO) as soon practically possible. It is especially important to report data breaches as promptly where there is low staff availability and or a Bank Holiday. The DPO will advise on whether to notify the ICO, however the final decision will rest with the organisation. If a decision to report is made, then it is the Organisation's responsibility to liaise with the ICO to ensure the report is sent off.

Notify data subjects (if necessary) if the breach is likely to result in a high risk to the rights and freedoms of individuals then you should promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach. When notifying individuals, you should consider including the following:

- Outline what has occurred and apologise
- Provide name and contact details of lead officer or relevant manager for further information
- Describe any likely consequences
- Describe any measures taken or proposed to be taken to address the breach including any measures to mitigate its possible adverse effects
- Advise whether the ICO has been notified
- Record notification to the data subject in breach log.

## **Monitoring and Compliance**

Compliance with this policy shall be monitored through a review process managed by the School Business Manager. All personal data breaches (and near misses) should be recorded whether or not they have been reported to the ICO. The breach log will include the facts of the breach, its effects and the remedial action taken. Staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken.

### *Learning from experience*

The relevant manager should, in consultation with the DPO, undertake a review of existing controls to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review should consider:

- Whether policy controls are sufficient
- Whether the breach occurred due to system error or human error or both
- Whether training and awareness can be amended and/or improved (if a report to the ICO is made, they are likely to seek details of training that has been undertaken)
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- If *Learning from experience* to be disseminated to all staff (where possible without identifying the person responsible).

### **Links with Other Policies**

This policy should be read in conjunction with other relevant policies, including but not limited to:

- Data Protection Policy
- Staff Acceptable Usage Policy

## Appendix 1 – Data Breach Reporting Form

<b>1. About the incident</b>	
<b>Date and time of incident</b>	
<b>Where did the incident occur?</b>	
<b>Date (and time where possible) of notification to the organisation</b> <i>If there was any delay in reporting the incident, please explain why this was</i>	
<b>Who notified the organisation of the incident?</b>	
<b>Describe the incident in as much detail as possible, including dates, what happened, when, how and why?</b> <i>Identifying information should be anonymised for any reporting purposes.</i>	
<b>2. Recovery of the data</b>	
<b>What have you done to contain the incident?</b> <i>e.g. limiting the initial damage, isolating affected systems, notifying the police where necessary, providing support to affected data subjects</i>	
<b>Please provide details of how you have recovered or attempted to recover the data, and when</b> <i>Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it</i>	
<b>3. About the affected people (the data subjects)</b>	
<b>How many individuals' data has been disclosed?</b>	
<b>Are the affected individuals aware of the incident, and if so, what was their reaction?</b>	
<b>When and how were they made aware / informed?</b>	
<b>Have any of the affected individuals made a complaint about the incident?</b>	

<b>Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?</b>	
<b>Your Organisation:</b>  <b>Your name and contact details:</b>	

## Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the head teacher and DPO and complete a data incident report available from the school office. The member of staff must also take appropriate mitigating action to minimize the impact of the breach and detail this in the data incident report.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the head teacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is 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.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. 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

As above, any decision on whether to contact individuals will be documented by the DPO.

- The DPO will 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 relating to the breach
  - 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 head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible