Holy Rood Catholic Primary School
Data Breach Procedure

Mission Statement

Live, Love, Learn

Holy Rood is proud to be a Catholic school, where Christ is at the heart of our community.

Working in close partnership with the home and parish, we share and celebrate our faith, while respecting and accepting those from other traditions and cultures.

We acknowledge each person's uniqueness and aim to provide a happy Christian environment where everyone can thrive.

We are committed to delivering a broad and balanced education, where each child can become the best they can be. We seek to nurture self-esteem in everyone and develop a sense of responsibility for ourselves and others.

We strive for excellence in all we do.

The purpose of this policy is to ensure that the school has a clear response to any reported data breach, ensure they are appropriately logged and managed in accordance with best practice guidelines, ensure any breaches are contained, risks associated with the breach minimized and actions considered to secure personal data and prevent further breaches.

Legal Framework

This policy has due regard to all relevant legislation and guidance, but not limited to, the following;

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Information Asset Management Policy
- Records Management Policy
- Secure Configuration Policy (Cyber Security)
- Ransomware Policy (Cyber Security)
- Password Policy (Cyber Security)
- Patch Management Policy (Cyber Security)
- Information Security Policy (Cyber Security)
- IT Asset Disposal Policy (Cyber Security)
- Firewalling Policy (Cyber Security)
- Access Control Policy (Cyber Security)
- Anti-Malware Policy (Cyber Security)
- Complaints Policy

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 Headteacher/School Office Manager.

The Headteacher/School Office Manager will investigate the report and consult with the Data Protection Officer (DPO), Tim Pinto, and determine whether a breach has occurred. To decide, the Headteacher/School Office Manager with support from 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 Headteacher/School Office Manager will alert the chair of governors and the UK GDPR governor.

The Headteacher/School Office Manager 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 Headteacher/School Office Manager will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The Headteacher/School Office Manager, with support/guidance from 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 Headteacher/School Office Manager 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 Headteacher/School Office Manager must notify the ICO.

The Headteacher/School Office Manager 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 server in a protected file.

Where the ICO must be notified, the Headteacher/School Office Manager will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Headteacher/School Office Manager 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 individual dealing with the breach
- 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 Headteacher/School Office Manager 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 Headteacher/School Office Manager expects to have further information. The Headteacher/School Office Manager will submit the remaining information as soon as possible.
- The Headteacher/School Office Manager 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:
  - The name and contact details of the Headteacher
  - 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 Headteacher/School Office Manager 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 Headteacher/School Office Manager 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 server in a protected file. The DPO and Headteacher/School Office Manager will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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.

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 Headteacher/School Office Manager as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Headteacher/School Office Manager will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Headteacher/School Office Manager will 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 Headteacher/School Office Manager will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The Headteacher/School Office Manager 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

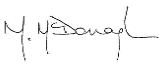
Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school web-site
- 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

Monitoring and Review

This policy will be reviewed on an annual basis by the governing board and headteacher.

Any changes to this policy will be communicated to all staff members and relevant stakeholders.

Approved by Chair of Governors 

Approved Date: 26 April 2024 Review Date: 25 April 2025