Approved:	November 2024
Review Date:	November 2025

POLICY DOCUMENT

Data Breach Response Plan

Information Governance (IG) Services.

ST JOHN BOSCO CATHOLIC ACADEMY

Contents

1 Data Breach Response Plan

1.1 Rationale

To ensure all personal and confidential information that the St John Bosco Catholic Academy holds is kept secure at all times in accordance with the Principles of the Data Protection Act 2018.

Under Article 5 Principles relating to processing personal data, it mentions the importance of personal data being '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, the principle of 'integrity and confidentiality.'

The school as an organisation is the data controller, not individual governors, teaching staff or the Data Protection Officer. The school is therefore responsible for ensuring good practice when it comes to the management of its personal data.

Having a Data Breach Response Plan ensures that the school is demonstrating evidence to the principle of accountability under data protection law.

1.2 Objective

A data breach response plan enables St John Bosco Catholic Academy to respond quickly to a data breach. By responding quickly, St John Bosco Catholic Academy can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result. Therefore, the objective of the Data Breach Response Plan is as follows:

- **Meet the schools obligations under the UK Data Protection Act 2018 –** Under the UK Data Protection Act 2018, a school must take reasonable steps to protect the personal information that it holds. A Data Breach Response Plan focussed on reducing the impact of a breach can be one of these reasonable steps.

- **Limit the consequences of a data breach** – A quick response can reduce the likelihood of affected individuals suffering harm (reducing the risk to the rights and freedom of individuals). It can also lessen financial or reputational damage to the school that experiences the data breach.

- **Preserve and build public trust –** An effective data breach response can support stakeholder confidence in a school's respect for individual privacy, and the school's ability to manage personal information in accordance with Data Protection law expectations.

This plan will mitigate the risk of further unauthorized access, loss of, and damage to information during and outside of normal school hours.

A Data Breach Response Plan is an important security and privacy control and supports the school's Business Continuity Plan.

1.3 What constitutes a data breach

A Data Breach Incident is any real or suspected event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised person;
- The integrity of a system or data being put at risk;
- The availability of a system or information being put at risk;
- An Information Security Incident could relate to any breach of security or confidentiality.

Examples of data breaches are:

- Losing a computer/device with personal information on it e.g. IPad, Laptop, Memory stick
- Giving information to someone who should not have access to it – verbally, in writing or electronically
- Using someone else's user ID and password to access a computer system
- Loss of paper documents containing personal information

1.4 Rights and Freedoms of individuals

The UK GDPR (Article 33) requires a breach to be reported where it is likely to **result in a high risk to the rights and freedoms of individuals**. Article 33 (4) does allow information to be provided in phases, as long as this is done without undue further delay.

Whilst there is no expectation that a full investigation will be carried out within 72 hours if it is considered there is a high risk to the rights and freedoms of individuals as a consequence of a breach, the school should still try to investigate within 72 hours of becoming aware of it. If the school

can't, it can explain to the ICO that it does not have all the relevant details but will have the results of the investigation in a few days. The investigation should be prioritised and given adequate resources.

Article 34 also make it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individual's rights and freedoms.

1.5 Factors to consider when a data breach occurs

Determining whether there is a high risk to the rights and freedoms of individuals the school must consider the following:

- **Whose personal information was involved in the breach?** The school should consider whose personal information was involved in the breach, as certain groups may be at particular risk of serious harm. If the data breach primarily relates to individuals known to be vulnerable, this may increase the risk of serious harm.

- **How many individuals were involved?** If the breach involves the personal information of many individuals, the scale of the breach should affect the schools assessment of likely risks. Even if the school considers that each individual will only have a small chance of suffering serious harm, if more people's personal information is involved in the breach, it may be more likely that at least some of the individuals will experience serious harm.

- **Do the circumstances of the data breach affect the sensitivity of the personal information?** A data breach involving an individual's name may involve a risk of serious harm if it contains sensitive information.

- **How long has the information been accessible?** The time between when the data breach occurred and when the school discovers the breach will be relevant to the school's consideration of whether serious harm is likely to occur.

- **Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible?** A relevant consideration is whether the information is rendered unreadable through the use of security measures to protect the stored information, or if it is stored in such a way so that it cannot be used if breached.

1.6 What to do when a data breach has occurred

Step 1: Contain the data breach to prevent any further compromise of personal information. Once a school has discovered or suspects that a data breach has occurred, it should immediately take action to limit the data breach.

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Addressing the following questions may help the school to contain a data breach:

(1) How did the data breach occur?
(2) Is the personal information still being shared, disclosed, or lost without authorisation?
(3) Who has access to the personal information?
(4) What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to mitigate any risk of harm.

An assessment of the data breach can help the school understand the risks posed by a data breach and how these risks can be addressed. It should be conducted as quickly as possible.

Gather and evaluate as much information about the data breach as possible. By creating a complete picture of the data breach, the school can ensure they understand the risk of harm to affected individuals and identify and take all appropriate steps to limit the impact of a data breach.

This assessment should also assist schools in deciding whether affected individuals must be notified. In the assessment of a data breach, consider:

- the type or types of personal information involved in the data breach
- the circumstances of the data breach, including its cause and extent
- the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

Step 3: Notify individuals and the Information Commissioner's Office if there is a high risk to the rights and freedoms of individuals.

Upon receipt of the completed security incident reporting form the YourIG Data Protection Officer service will make an assessment of the severity of the incident.

Following the assessment they will discuss with the school the outcome of the assessment and any actions that need to be taken by the school and whether the incident requires reporting to the ICO.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches. Once steps 1 to 3 have been completed, the school should review and learn from the data breach incident to improve its personal information handling practices. This might involve:

- a security review including a root cause analysis of the data breach.
- a prevention plan to prevent similar incidents in future.
- audits to ensure the prevention plan is implemented.
- a review of policies and procedures and changes to reflect the lessons learned from the review.
- a review and consideration of training within the school.
- a review of any partners that were involved in the breach.

1.7 Data Breach Response Team

In the event of a serious data breach the school will need to convene a Data Breach Response Team. This may include members of SLT, the school's DPO and a member from the school's IT Team to assist in the further investigation of the incident, including the extent of the incident and whether any steps need to be taken to contain any breach.

1.8 Further Information

The Data Breach Response Plan should be read in conjunction with the following documents:

- Dealing with a Security Incident Guidance
- Information and Cyber Security Policy
- Ransomware and Data Protection Guidance

Further advice and assistance around any Information Governance matters (including for example Data Protection, data security and FOI requests) is available to schools by contacting the school's Data Protection Officer (DPO)].

James Gray -
Dudley MBC, The Council House, Dudley, DY1 1HF
Email: james.gray@dudley.gov.uk tel: 01384 815607

1.9 Reporting a Data Breach Plan (Appendix 1)

Question	Response
Date and time this record was completed	
Name of person completing this record	
General description of the breach	
Name and job title of person who originally reported the breach / suspected breach	
Date and time the breach / suspected breach was reported	
Who was the breach / suspected breach reported to?	
Has the Data Protection Officer been informed?	
Has the members of SLT been notified?	
What are the details of the breach / suspected breach (include as much detail as possible) NB: An investigation must be undertaken where appropriate	

Who is responsible for the breach i.e. the school as data controller, a joint data controller or a data processor? Is the breach ongoing or has it been contained?	
Is any other information required in order to assess the extent of the breach / the risk to data subjects? If so, specify that information here.	
Whose data has / may have been compromised as a result of the breach / suspected breach?	
Type of data involved in the breach / suspected breach	
Does the breach / potential breach involve sensitive personal data or information about criminal offences?	
What is the likely risk to individuals?	
Is there likely to be a high risk to individuals?	
Does the breach need to be reported to the ICO? If yes, and if the breach happened more than 72 hours ago, what is the reason for the delay if notifying the ICO?	YourIG will triage the data breach and notify the school whether it is reportable or not

If the breach has already been reported to the ICO, confirm the date and time the report was made, who made the report and whether the report was made within 72 hours	
If a report has been made to the ICO, what advice or recommended actions have been given? Specify any sanctions that are issued by the ICO following a breach.	This will be provided by the ICO Case Officer assigned to review the data breach
If a report to the ICO is not being made, confirm the reasons why and whether the decision needs to be kept under review	
Do the data subjects affected need to be notified about the breach? If so, confirm who will notify them and how and when they will be notified. If data subjects are not going to be informed, explain the reasons why.	
Does the breach need to be reported to the Police?	
Has the school reported the data breach to Action Fraud?	
Do any other steps need to be taken e.g. comms to stakeholders, provision of complaints policy, consult legal advisors, notify insurers, external IT support.	
Is there likely to be press / media interest as a result of the breach? If so, have the appropriate protocols for handling media enquires been followed?	

Outline the actions that need to be taken in response to the breach / suspected breach to reduce the risk of a re-occurrence and who is responsible for implementing them and the relevant timescales. This should include whether an investigation under the school's disciplinary policy is recommended. NB: The information provided in response to this question is likely to be a summary as a more detailed report / audit is likely to be required following a data breach which is notified to the ICO	