Appendix 5

Saint Robert Lawrence Catholic Academy Trust
Data Breach Procedures

This procedure is designed to ensure that all staff, governors and directors are aware of what to do in the event of a DPA / GDPR breach and that they need to act swiftly to report the breach. The attached 'Data Breach Flowchart' outlines the process.

The Trust recognises that most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, laptop, USB memory stick or similar
- Sending an email with personal data to the wrong person or to too many people who may not need to or be entitled to see the data
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to the Trust's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What should staff do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter. Report the breach to the Data Controller and Data Protection Officer as soon as possible, this is essential.

What will happen next?

The breach notification form will be completed and the breach register updated. The breach report to the ICO will be submitted within 72 hours of the Data Controller becoming aware of the breach.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.
It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Breach notification to data subject
For every breach the Trust will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Officer.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection
It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as part of an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of the Trust, which may be the er or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Evidence Collection Log

Date	Evidence Description	Secure storage location & confirmed date	Trust Officer

Data Breach Notification Form

When did the breach occur (or become known)?	
Who was involved in the Trust?	
Who was this reported to?	
Date and time it was reported	
Date and time DPO notified	
A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI numbers	
The categories of personal data affected – electronic, hard copy	
Approximate number of data subjects affected.	
Approximate number of personal data records affected.	
Name and contact details of the Data Protection Officer / GDPR Owner.	
Consequences of the breach. What are the potential risks?	
Any measures taken to address the breach. What actions and timeline have been identified?	
Any information relating to the data breach.	

Breach Management Flowchart