POLICY

Type of Policy:	MAT Policy to adopted in full across all schools LGB Policy to be reviewed and approved locally	✓

Approval Date:	**2022/23 - SUMMER TERM (TB)**
Review Date:	**2023/24 – SUMMER TERM**

SOUTH EAST LONDON CATHOLIC ACADEMY TRUST (SELCAT)

DATA BREACH POLICY

Our Vision, Mission & Values

To create a family of schools that together, through shared support and challenge, strive to provide an authentic Catholic education where all children will be empowered, inspired and flourish.
We will aim for excellence and to become remarkable places of learning and love.

Introduction

We recognise that a breach of personal data could happen, despite our policies, procedures, and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm, to the school or to individuals.

This procedure supports our Data Protection Policy. It includes our guidelines for reacting to and handling any breach, or suspected breach, or personal data, in line with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and best practice.

Scope and Responsibilities

This policy applies to all instances when it is known or suspected that personal data that the school handles has been subject to a breach (see below for breach definition.)

All staff are responsible for reading, understanding, and complying with this policy.

Our Data Protection Officer provides assistance and further guidance on data breaches. The Data Protection Officer is responsible for taking the lead on the steps in this procedure once a breach, or suspected breach, has been reported internally.

Any staff member becoming aware of a breach is responsible for immediately reporting it internally, to ensure it can be handled appropriately.

What is a Personal Data Breach?

If personal data we handle is lost, destroyed, altered, disclosed, accessed, or put beyond use when it shouldn't be, this is a Personal Data Breach. This procedure will be followed as soon as we become aware of a breach.

Where we suspect personal data has been subject to a breach, we will follow this procedure until we are sure of the status of the personal data.

A personal data breach can occur accidentally or intentionally, by staff, or anyone else.

Breach Response Plan

All members of staff are responsible for taking all reasonable steps and cooperating with key staff in following this procedure when a breach is found or suspected.

The breach response plan has 7 steps, which are covered in detail below:

1. Report the breach internally
2. Assess the risk
3. Contain and recover
4. Notify the ICO of the breach (if applicable)
5. Notify the affected Data Subjects of the breach (if applicable)
6. Review
7. Implement any necessary changes to prevent reoccurrence

1. Report the Breach Internally (School Staff)

As soon as you become aware of a breach, or possible breach, report it to the Head Teacher, or another senior staff member in their absence, who will lead on the breach response, and inform the Data Protection Officer of the breach and keep them updated on the investigation and actions as appropriate.

The report should be made as soon as possible even if the breach is discovered outside of normal working hours.

2. Assess the Risk (DPO)

The DPO will consider what harm could come from the breach, including who could be harmed, how they could be harmed, and how severe the harm could be, as well as how likely is the harm to happen. This risk assessment, based on severity and likelihood, will depend on the types of information involved (how sensitive is it, what could be done with it?), how much information is involved, and how exposed the data is, as well as the individual circumstances of the data subjects (people the data is about.)

As an example, if a laptop has been lost, if it is encrypted there is a very small chance of any data being accessed. But if hard copy documents have been lost or left unattended, they are much more likely to be accessed and read.

As another example, if personal data is included in an email by accident, the data may be at more risk of being misused if the email has gone to a member of the public, rather than to another school.

As an example, regarding the data subjects' circumstances, accidentally disclosing an address might not pose a risk to most data subjects, but it could be very high risk for someone who is escaping domestic violence, or for the adoptive family of a child.

3. Contain and Recover (School with DPO Support)

Take reasonable actions to contain the risks, and/or recover the data, if possible. Containment and recovery actions could include, as appropriate:

- Attempting to find lost devices or paperwork
- If devices have been stolen, report this to the police
- If a breach is still occurring, for example, due to an ongoing IT issue, then IT should take appropriate steps to minimise the breach, such as closing down an IT system. In the event of a Cyber attack, immediately report to the Action Fraud line on 0300 1232040.
- Warning staff and third parties to be aware of any "phishing" attempts that might be linked to personal data that has been accessed by criminals/unauthorised people
- If data has been sent to, or shared with, someone it shouldn't have been, consider if you can contact them to recover the data. Bear in mind that "recall" doesn't usually work on externally sent emails
- If bank details have been lost/stolen, contact banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

4. Notify the ICO of the Breach (DPO)

Breaches that could cause a risk to people should be reported to the Information Commissioner's Office (the ICO – the UK's data protection regulator) and, in some cases, to the data subject(s) involved too.

Not all breaches will need to be reported. For example, if data is deleted in error, it is technically a breach, but if the data is backed up and can be promptly reinstated, it does not represent a risk to data subjects.

If the DPO decides not to report a breach to the ICO and/or the data subjects involved, the decision and reasons will be recorded.

If it is likely the breach will result in a risk to people's rights and freedoms, and have an adverse effect on data subjects, causing them harm, it must be reported to the ICO.

Reports to the ICO must be made within 72 hours of us becoming aware of the breach. Information can be provided to the ICO in stages, giving them the details as and when we find out more, but the first contact must be within 72 hours.

- The information to be provided to the ICO:
- A description of the personal data breach that has occurred including, where possible:
  a) the types and approximate number of people whose data is involved
  b) the types and approximate number of personal data records involved
- The likely consequences of the breach
- The measures taken, or proposed to be taken, in response to the breach, including actions to mitigate any possible harm to data subjects
- The name and contact detail of the Data Protection Officer, or any other contact details of people who can provide more information.

5. Notify the Affected Data Subjects of the Breach (DPO)

If the risk to data subjects is assessed as high, the breach must also be reported to everyone whose data is involved, to allow them to take any appropriate steps to protect themselves and so they are aware of anything that may happen. For example, if financial information has been lost or stolen, they can alert their bank for fraudulent activity, or if passwords have been lost or stolen, they can change them on their accounts and any other accounts that they used the same password on.

We can choose to report to data subjects even if the risk is not high, if we consider it would be better for us to tell them about the breach for other reasons, such as supporting transparent relations and trust.

6. Review

The review stage includes reviewing and evaluating the response to the breach. Consider how effective the response was, and if improvements could be made when handling any future breaches.

As examples, did the person who first became aware of the breach know to report it internally? Did attempts to recover the data work? How could the breach have been handled better or quicker?

The breach, and outcomes of the review, should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then

an action plan will be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation will liaise with the CEO for advice and guidance.

7. Implement Any Necessary Changes to Prevent Reoccurrence

Depending on how the breach occurred, actions should be taken to reduce the risk of something similar happening, including amongst other things, improved IT security, new or improved written procedures, refresher training, improved supervision, changes to processes, communications to remind colleagues about risks, etc.

Other steps to minimise data breaches should include:

- Staff are actively encouraged to use Trust/School cloud services for the secure storage of school information rather than USB sticks. Only where there are restrictions to do so, will data sticks be permitted, and they must be encrypted.
- Regular training of all staff is to ensure that awareness remains high so that privacy by design and privacy by action can minimise data breach risks.
- Staff are reminded routinely to lock their computer screens when away from their desks.
- Staff are reminded not to include pupil names in email subject headers.

Data Breach checklist

Action	**Give dates, initials, and links to docs where appropriate**
Date and time of discovery	
Date and time of occurrence	
What happened	
Immediate steps taken to contain the breach, e.g. changing passwords, shuttingcomputers down, halting network traffic, restore data from backups	
Acknowledge breach by thanking informant for information – log it here	
Inform DPO	
Assess Risk:	[Consider how many people are affected, what type of data is involved, how could people be harmed, and how likely are they to be harmed?]
Necessary to inform ICO? 0303 1231113	
Date and time reported to ICO	
Necessary to inform data subjects?	
Data subjects informed?	
Police informed?	
Review:	[Consider what was in place that should have prevented the breach, and why it failed, how could further breaches be prevented, how havewe helped the people effected? Should we improve security, procedures, training, etc?]