

St Luke's C of E Primary School

Data Breach Procedure

Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

Breach Notification

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify Calum Howard via office@stlukeslondon.org. If you are an internal member of staff please email Mr. Howard directly. They will make a decision whether to refer the matter to the Data Protection Officer (DPO) Jay Makwana (jay.makwana@london.anglican.org or 020 3837 5073.

Irrespective of whether the DPO is notified or not the response to the breach will follow the same path and be be broken down into four distinct sections: **Investigation, Recovery, Reporting, Remedial Action.**

Investigation, Recovery and Reporting must be undertaken within **72hrs** of breach realization. Remedial Action must be considered and decided on within this time frame but does not need to be fully enacted. 72hrs is the period of time which Data Protection Act 2018 allows for referral to the ICO or Data subjects.

Stage 1: Investigation:

All suspected breaches will be entered onto the "Data Breach Log" and assigned a unique reference number. All subsequent information will then be recorded on this log.

In addition, where required a corresponding file should be opened named after the unique reference number. All articles relating to the investigation, recovery and reporting should be stored within this file.

The first stages of the investigation into the breach report is to determine whether a breach has occurred by deciding if personal data has been accidentally or unlawfully mishandled. This will be done by assessing whether the data has been:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorized people

If a breach has been confirmed, then the severity of it will be assessed by considering:

- Data subject affected (vulnerability)Number of Data subjects affected.
- Data type lost, personal identifying/ special category,
- Specific Data Sets lost
- Number of Data sets
- Format of Data, electronic/paper.

Stage 2 Recovery:

The next stage is to contain and minimize the impact of the breach, this will be assisted by relevant staff members or data processors where necessary.

This may include but not be limited to:

- Contacting parties who may have received the data.
- Email Recovery
- Backup file restoration
- Requesting deletion of data.

If the data has been sent to the wrong individual and it has been requested to be deleted, confirmation of deletion should be attained in a written format for posterity.

The success or failure of the recovery must be recorded and will inform the reporting stage.

Stage 3: Remedial Action.

Once the details of the breach are known and as the recovery process is being undertaken an assessment needs to be made on what potential future action could be considered to prevent a similar breach reoccurring.
This will involve reviewing the processes and procedures which may have failed resulting in the breach.

Potential remedial actions may include, but are not limited to:

- Anonymizing and minimizing data
- Encrypted drives
- Secure access servers
- Strong password setting
- Training and support for staff and governors
- Encrypted email

All potential remedial action is to be recorded on the Data Log.

Stage 4 Reporting:

The investigator must decide who should be informed about the breach, affected data subjects and/or the ICO.

For Cyber Security or Fraud related breaches a referral to Action Fraud or National Cyber Security Centre may also be warranted.
Depending on the result of the containment efforts, the investigator will review the potential consequences, assess their seriousness and likelihood then make a decision about who needs to be informed. This will be partly determined by assessing if the risk of damage caused by the breach exceeds that of the damage that may be caused to the relationship through being informed.

If the risk of personal damage exceeds that of relationship, the Data Subjects will be promptly informed, 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

The decision on whether to contact individuals will be documented.

A decision also needs to be made if the breach has reached the threshold to be reported to the ICO. This must be judged on a case-by-case basis.
To decide, the investigator will consider whether the breach poses a significantly risk 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
- Unauthorized reversal of pseudonymization (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 decision will be documented 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 ***Place Decisions are documented***

Where the ICO must be notified, this will be done 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 reporter will set out all known details of the breach including recovery attempts and their success. Potential remedial action will be included if known.

If all the breach details are not yet known, then as much as is known should be reported to the ICO within 72 hours. The report will explain that there is a delay, the reasons why, and when the further information is expected to be known. Then the remaining information will be submitted as soon as possible

At the conclusion of all stages of the Data Breach a mini report can be supplied to the Headteacher and Governors to brief them the outcome and propose ways it can be prevented from occurring again.
This is to allow Governors to hold the school accountable as per the Accountability Principle.