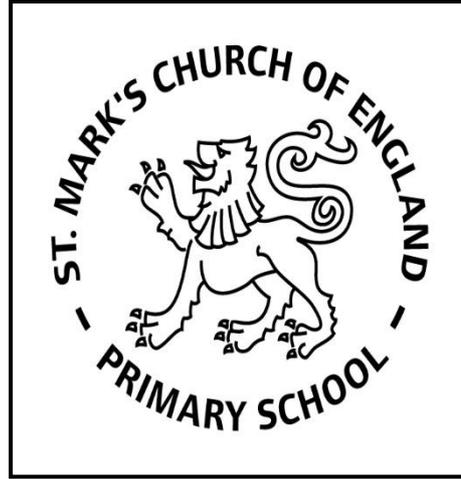


# Breach Management Policy



'Thy Word is a Lamp to my Feet  
and a Light to my Path'  
Psalm 119 v 105

"Every Child, Every Chance, Every Day"



**Every Child, Every Chance, Every Day**

## **Breach Management Policy**

Governors and staff are committed to delivering the very best for our children. Our Vision is fundamental to our role as a Church of England School with its roots coming from the original blessing and verse presented to our school on its official opening in 1955.

***Thy word is a lamp to my feet and a light to my path.***

*Psalm 119 Vs 105*

*The following five components describe the desired outcomes we offer through it.*

- *Together, we will prepare you for life and learning*
- *Together, we will teach you to live within the values of God's word*
- *Together, we will safely lead you on your journey*
- *Together, we will guide you to a fulfilling future*
- *Together, we will forever help you to grow in confidence*

### **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 **Karen Kean – School Admin & Finance Manager** at **02072725967**

They will make a decision where to refer the matter to the Data Protection Officer (DPO) **Claire Mehegan** [claire.mehegan@london.anglican.org](mailto:claire.mehegan@london.anglican.org)

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

Investigation, Recovery and Reporting must be undertaken within **72hrs** of any staff member or processor becoming aware of the breach. This is the period of time which the Data Protection Act 2018 allows for referral to the ICO or data subjects.

### **Stage 1: Investigation:**

Investigation into the breach report 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

Once 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/etc)

Once a breach has been confirmed, it will be entered onto the “Data Breach Log” and assigned a date and/or unique reference number. All subsequent information will then be recorded on this log.

In addition, for complex breaches a file folder should be opened named after the unique reference number. All articles relating to the investigation, recovery and reporting should be stored within this folder.

### **Stage 2 Recovery:**

Next stage is to contain and minimize the impact of the breach, 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 action the next stage.

### **Stage 3 Reporting:**

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

- Depending on the result of the containment efforts, the investigator will review the potential consequences, assess their seriousness and likelihood then decide who needs to be informed.

If the risk of harm is high, all data subject(s) whose personal data has been affected will be promptly informed, in writing. The breach 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.

Whether the breach must be reported to the ICO must be judged on a case-by-case basis.

To decide, the DPO 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
- 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

1. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
2. 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 ***on a password protected drive.***
3. 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 DPO will set out:

4. If all the above 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

**Stage 4: Remedial Action.**

Finally, the breach will be assessed, and potential future actions considered on how to prevent a similar breach reoccurring.

Such actions 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

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 a recurrence of such a breach can be prevented.

This is to allow Governors to hold the school accountable as per the Data Protection Principle of accountability.

Reviewed and ratified by Governing body	Spring Term 2021		
Next Revision (Please highlight as appropriate)	<b>Annual</b>	Biennial	Tri-annual
To be reviewed	Spring Term 2022		