

POLICY TYPE: PRESCRIBED
ACTION: FOR SCHOOL ADOPTION

Approval Body: SDBEMAT BOARD
Approval Date: SEPTEMBER 2024
Version: 6 (SEPTEMBER 2024)
Policy Ref: GDPRPHDBL



**Southwark Diocesan
Board of Education
Multi-Academy Trust**
Developing Church of England Education

GDPR POLICY HANDBOOK

DATA BREACH LOG

DATA BREACH LOG

This Data Breach Log must be completed by a suitably trained person following any reports of a security breach or suspected breach involving personal data.

Staff must follow the Trust's Data Breach Response Plan following notification of a breach or suspected breach. In the event you are unsure whether to notify the ICO and the data subjects, you should obtain legal advice without delay as the ICO must be informed about notifiable breaches within 72 hours.

Information	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 Data Breach Response Team been notified?	
What are the details of the breach / suspected breach (include as much detail as possible)	

Information	Response
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?	

Information	Response
<p>If yes, and if the breach happened more than 72 hours ago, what is the reason for the delay if notifying the ICO?</p>	
<p>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</p>	
<p>If a report has been made to the ICO, what advice or recommended actions have been given?</p> <p>Specify any sanctions that are issued by the ICO following a breach.</p>	
<p>If a report to the ICO is not being made, confirm the reasons why and whether the decision needs to be kept under review</p>	
<p>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.</p> <p>If data subjects are not going to be informed, explain the reasons why.</p>	
<p>Does the breach need to be reported to the Police?</p>	
<p>Do any other steps need to be taken e.g. communications to stakeholders, provision of complaints policy, consult legal advisors, notify insurers, external IT support.</p>	

Information	Response
<p>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?</p>	
<p>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.</p> <p>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.</p>	

CONTACT DETAILS

Mark Burnett, Chief Operating Officer & DPO,
 mark.burnett@southwark.anglican.org

Thomas Scrace, HR Business Partner & Deputy DPO,
 thomas.scrace@southwark.anglican.org

SCH LEAD, Deputy Head,
 SCH LEAD EMAIL

[INSERT CONTACT DETAILS FOR EXTERNAL ORGANISATIONS WHO MAY NEED TO BE INVOLVED IF THERE IS A DATA SECURITY BREACH]

