Overleigh St Mary's C of E Primary School

Data Breach Policy

Signed by:

	Head teacher	Date:	Summer 2024
	Chair of governors	Date:	Summer 2024

Data Breach Policy

Data Protection - Data Breach Procedure

Overleigh St Mary's CE Primary School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held at Overleigh St Mary's CE Primary School. This procedure applies to all school staff including governing bodies, referred to herein after as 'staff'.

Purpose
This breach procedure sets out the course of action to be followed by all staff at our school if a data protection breach takes place.

Legal Context
The General Data Protection Regulation 2018 makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Principle 7 of the Act states that organisations which process personal data must take
"appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

Types of Breach
Data protection breaches could be caused by a number of factors. Some examples are:
 Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
 Inappropriate access controls allowing unauthorised use;

 Equipment Failure;
 Human Error;
 Unforeseen circumstances such as fire or flood;
 Hacking;
 ‘Blagging’ offences where information is obtained by deception.

Immediate Containment/Recovery
In discovery of a data protection breach, the following steps should be followed:
1. The person who discovers/receives a report of a breach must inform the Head Teacher or Amanda Beaumont who will inform the DPO Sarah Webb. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The DPO must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school’s responsibility to take the appropriate action and conduct any investigation. However, should the Head Teacher (or nominated representative) require any expert guidance and assistance; they can contact the Data Protection Officer.

4. The DPO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5. The DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries (‘phishing’) for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer’s name and contact details if possible and confirm that they will ring the individual making the enquiry back.

Whatever the outcome of the call, it should be reported immediately to the DPO.

d. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. 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.

Investigation
In most cases, the next stage would be for the Head Teacher (or nominated representative) to fully investigate the breach. The Head Teacher (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:
 The type of data;
 Its sensitivity;
 What protections are in place (e.g. encryption);
 What has happened to the data;
 Whether the data could be put to any illegal or inappropriate use;
 How many people are affected;
 What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed to within 72 hours to meet the GDPR criteria. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification
Some people/agencies may need to be notified as part of the initial containment.. The DPO should, after seeking expert or legal advice, decide whether anyone should be notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) should be notified.

Every incident should be considered on a case by case basis in by the DPO, who will assess the severity of the breach and what actions need taking, including escalation to ICO.

Review and Evaluation

Once the initial aftermath of the breach is over, the DPO should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available Management Team meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the data protection policy is reviewed.

Implementation

The Head teacher should ensure that staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction and supervision. If staffs have any queries in relation to the policy, they should discuss this with their line manager or the Head Teacher.