Data Breach Process

December 2025

Data Breach Process

Although The Mayflower Primary School takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the <school/academy>

However the breach has occurred, the following steps should be taken immediately:

1. **Internal Notification:** Individual who has identified the breach has occurred must notify The Mayflower Primary School GDPR Officer or Headteacher. A record of the breach should be created using the data breach form.

2. **Containment:** GDPR Officer/Headteacher to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. **Recovery:** DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, backup tapes to restore lost or damaged data).

4. **Assess the risks:** Before deciding on the next course of action, DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form (Appendix C):

    a. What type of data is involved
    b. How sensitive is it?
    c. If data has been lost/stolen, are there any protections in place such as encryption?
    d. What has happened to the data?
    e. What could the data tell a third party about the individual?
    f. How many individual's data have been affected by the breach?
    g. Whose data has been breached?
    h. What harm can come to those individuals?
    i. Are there wider consequences to consider such as reputational loss?

5. **Notification to the Information Commissioners Office (ICO):** Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

    The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. **Notification to the Individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the Mayflower Primary School.

7. **Evaluation:** The DPO should assess whether any changes need to be made to the Mayflower Primary School's processes and procedures to ensure that a similar breach does not occur.

Mayflower Primary School

Data Breach Incident Report Form

Please complete form and return it to the GDPR officer/Head teacher ASAP

<table>
<tr><td>Description of Data Breach
(i.e. Laptop stolen from vehicle)</td><td></td></tr>
<tr><td>Time and date the breach occurred (if known)?</td><td></td></tr>
<tr><td>Time and date the breach was discovered, by whom and how was it discovered?</td><td></td></tr>
<tr><td>Who is reporting the breach?</td><td></td></tr>
<tr><td>Contact details
(Telephone/email)</td><td></td></tr>
<tr><td>What type of personal data was included in the breach?

Mark ALL categories applicable (involved or potentially involved).

Very important:
If the data involved is in either the Sensitive or Confidential category, it must be reported to the GDPR Officer and Head Teacher immediately.</td><td>
<table>
<tr><td>Basic personal identifiers (Mr, Mrs etc.)</td><td></td></tr>
<tr><td>Contact information (telephone, email, address etc.)</td><td></td></tr>
<tr><td>Identification data (usernames, passwords etc.)</td><td></td></tr>
<tr><td>Other:</td><td></td></tr>
</table>
Basic Information

Special Category Data (Sensitive)
<table>
<tr><td>Data revealing racial/ethnic origin</td><td></td></tr>
<tr><td>Health data (medical/mental health)</td><td></td></tr>
<tr><td>Political opinions/affiliations</td><td></td></tr>
<tr><td>Trade Union membership</td><td></td></tr>
<tr><td>Religious/philosophical beliefs</td><td></td></tr>
<tr><td>Sex life data</td><td></td></tr>
<tr><td>Sexual orientation data</td><td></td></tr>
<tr><td>Gender reassignment data</td><td></td></tr>
<tr><td>Criminal convictions/offences</td><td></td></tr>
<tr><td>Genetic/biometric data</td><td></td></tr>
<tr><td>Other:</td><td></td></tr>
</table>
Confidential Data
</td></tr>
</table>

	<table><tr><td>Date of birth</td><td></td></tr><tr><td>National insurance number</td><td></td></tr><tr><td>Official documents (driving license, passport etc.)</td><td></td></tr><tr><td>Financial data (credit card details, bank details)</td><td></td></tr><tr><td>Location data</td><td></td></tr><tr><td>Other:</td><td></td></tr></table>
Number of personal data records involved.	
Number of data subjects that could be affected.	
Categories of data subjects involved. Mark **ALL** categories applicable (involved or potentially involved). **Important:** Vulnerable includes SEND, safeguarding concerns, mental health issues.	<table><tr><td>Pupil(s)</td><td></td></tr><tr><td>Ex Pupil(s)</td><td></td></tr><tr><td>Staff</td><td></td></tr><tr><td>Ex Staff</td><td></td></tr><tr><td>Parent/Guardian</td><td></td></tr><tr><td>Visitor</td><td></td></tr><tr><td>Potential Parent/Pupil</td><td></td></tr><tr><td>Vulnerable Pupil</td><td></td></tr><tr><td>Vulnerable Adult</td><td></td></tr><tr><td>Other:</td><td></td></tr></table>
Confirmed or Suspected breach?	<table><tr><td>Confirmed</td><td></td></tr><tr><td>Suspected</td><td></td></tr></table>
Potential consequences of breach?	
What is the likelihood that data subjects will experience significant consequences because of the breach?	<table><tr><td>Very likely</td><td></td></tr><tr><td>Likely</td><td></td></tr><tr><td>Unlikely</td><td></td></tr><tr><td>Very unlikely</td><td></td></tr><tr><td>Not yet known</td><td></td></tr></table>
Reason likelihood was selected?	
Is the breach contained or ongoing?	<table><tr><td>Contained</td><td></td></tr><tr><td>Ongoing</td><td></td></tr></table>
If ongoing, what actions are being taken to recover data?	

Who has been informed about the breach?	
Any other relevant information	

Investigator Only

Received by:	
Date/Time:	
Classification of data breach	<table><tr><td>Public data</td><td></td></tr><tr><td>Internal data</td><td></td></tr><tr><td>Confidential data</td><td></td></tr><tr><td>Special category data</td><td></td></tr><tr><td>Vulnerable group data</td><td></td></tr><tr><td></td><td></td></tr></table>
Data breach status	<table><tr><td>Reportable to ICO?</td><td></td></tr><tr><td>Reportable to the ICO and data subjects?</td><td></td></tr><tr><td>Recordable on B1 template only?</td><td></td></tr><tr><td></td><td></td></tr></table>
ICO identification details	<table><tr><td>ICO number</td><td></td></tr><tr><td>ICO breach incident number</td><td></td></tr><tr><td>Update required?</td><td></td></tr></table>
Remedial action required?	
What remedial action is being carried out and by whom?	
Data subject risk grid required?	
Who is creating the data subject risk grid?	

DPO Comments	
