Data Breach Policy

Policy Monitoring, Evaluation and Review

This policy is effective for all schools within The Mead Educational Trust, the Teaching School, the SCITT and all other activities under the control of the Trust and reporting to the Trust Board.

Version	4.0
Date created	April 2024
Author	GDPR Sentry
Ratified by	Executive Team
Date ratified	30 April 2024
Review date	April 2026

Revision History:

Version	Date	Author	Summary of Changes:
4.0	April 2024	CBR	Changed GDPR to UK GDPR because the UK has left the EU and has formed its own data protection legislation.
3.0	April 2022	GDPR Sentry	Adopted new policy from external DPO service to reflect data management practices
2.0	Nov 2020	CBR	Policy reviewed, no changes
1.0	July 2018	CBR	New policy

Contents

1 Purpose

The Mead Educational Trust ("the Trust") is required to follow the Data Protection Act (2018) ("the Act") in the way that it collects and uses personal data. The Act references and implements the UK General Data Protection Regulation (GDPR) with some specific amendments. Section 2 of Chapter IV of the UK GDPR sets out the requirements for data controllers to implement appropriate security measures and how personal data breaches should be notified.

This policy sets out the approach that the Trust will take to deal with personal data breaches.

This policy applies to:

- All employees of the Trust
- All those involved in governance (e.g. Trustees, academy councillors)

The Data Protection Officer is GDPR Sentry Limited.

2 Introduction

The UK GDPR describes the responsibilities that organisations have when dealing with personal data. Personal data is defined as any information relating to an identified or identifiable natural person. The person is known as a 'data subject'.

The sixth principle of data protection states that personal data shall be *'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.'*

Notwithstanding the measures that Data Controllers put in place, it is inevitable that sometimes a failure will occur with respect to this principle, creating a personal data breach. Three types of breaches are recognised:

- Confidentiality – unauthorised access or use of personal data
- Availability – personal data that should be available is not accessible
- Integrity – inaccurate personal data has been recorded

In the event of a data breach, there are a set of key actions which must be undertaken.

3 Related policies

This policy is closely linked with other policies which should be referenced when appropriate, including:

- Data Protection Policy
- Any other relevant guidance documents

4 Responsibilities

4.1 The Trust will:

4.1.1 Put in place a clear procedure for dealing with personal data breaches. This procedure should take account of the requirements laid down in Annex 1.

4.1.2 Follow any additional guidance from the Information Commissioner's Office (ICO) produced subsequently to this policy.

4.1.3 Inform the Data Protection Officer of all personal data breaches (by logging them on GDPR Sentry).

4.1.4 Record the details of personal data breaches and make those records available to the Data Protection Officer (via GDPR Sentry).

4.1.5 Ensure that personal data breaches are dealt with in line with the statutory time limits and notify the Data Protection Officer as soon as possible if these limits cannot be met.

4.1.6 Take advice from the Data Protection Officer with regards to the management of personal data breaches.

4.2 The Data Protection Officer will:

4.2.1 Provide guidance and support to the Trust in dealing with a personal data breach.

4.2.2 Provide a route of communication to the Information Commissioner's Office in the event of notification being required and any follow-up actions.

Annex 1: Procedure for managing personal data breaches

1. Responsibilities

Data breaches have 72 hours in total (from the point of detection) to be investigated, mitigated and assessed with respect to the need for notification to the Information Commissioner's Office (ICO). It should be noted that this is 72 elapsed hours including weekends and holidays.

Potential or actual data breaches pose the greatest threat in terms of financial penalty to the Trust and to its wider reputation. It is arguable that for the Trust the reputational damage is a greater risk than any potential fines.

This being the case, the management of personal data breaches needs to be managed by senior staff who are able, without restriction, to bring about immediate mitigation of a potential or actual breach.

The Trust Data Protection Lead will manage the response to a data breach at Trust level and will include staff from Operations, IT and HR, as required. If the breach relates to a school, the school's Data Protection Lead will be involved.

The Data Protection Officer will need to be immediately informed and advise on actions to be taken on any potential or actual data breach.

2. Procedure overview

The procedure for managing personal data breaches needs to take account of the following stages and requirements. The actions described in this section are by no means exhaustive.

I. Discovery of a personal data breach

II. Investigate the nature of the breach

III. Action to contain the breach

IV. Assess the level of notification required

V. Notify appropriate parties

VI. Identify actions to minimise the reoccurrence of the breach

3. Discovery of a personal data breach

This section covers both the initial recognition that a breach has occurred and the notification to enable action to be taken.

Any member of staff at the Trust may identify that a breach has potentially occurred. They may also receive a report from a pupil or any other stakeholder that a potential breach has occurred. Section 9 of this annex lists some circumstances that, upon discovery, point to a likely data breach. It is essential to recognise that these are for guidance and illustration only. If in doubt, inform the Data Protection Lead of the Trust or school.

Reporting a breach makes a positive contribution to the Trust in managing its data protection responsibilities.

Although not all personal data breaches are reported to the Information Commissioner's Office,

each incident should be treated as though it might be until the evidence shows otherwise.

It is, therefore, essential that when a potential breach is discovered that it is reported as soon as possible.

The Trust has provided the email address **dpo@tmet.uk** for communications about data protection issues and this email address is checked outside of normal working hours and outside of term time. Alternatively, staff have a login to GDPR Sentry and can log a data breach via that platform, which sends an automatic notification to the Data Protection Leads of the Trust and school.

As mentioned in Section 1, in the case of a personal data breach that must be reported to the ICO, there is a 72-hour window. It should be noted that at the point any member of staff becomes aware of a potential breach this is the start of the 72-hour window, not when the Data Protection Lead or the DPO is informed.

For example, if a member of staff discovers that their car been broken into on Friday evening and a laptop is stolen, this is the discovery of the breach, not when it might be reported to the Trust after the weekend.

Members of staff are not expected to independently investigate potential breaches before bringing them to the attention of the Data Protection Lead as this will reduce the time available for management of the issue.

Information required when reporting a breach

From the initial report, it is essential to establish a chronology for the breach. This will later include information about actions taken and impact assessments. At this first stage the person reporting the breach needs to provide:

a. The time and date that the suspected breach was detected.

b. A description of the nature of the breach including classification (Confidentiality, Availability, Integrity).

c. The data subjects, types of personal data and number of records affected.

d. How the individual identified the potential breach.

e. Details of any individuals they have discussed the potential breach with.

If there are emails or other notes, call records or any other materials associated with the discovery of the breach, these should be provided although it is recognised that there may be a delay in assembling all the material.

It should be noted that, depending on the exact circumstances, the person who has identified the potential breach may have minimal information.

4. Investigate the nature of the breach

The core focus at this stage is to have enough information to determine if notification to the ICO will be required. The report from the individual who discovers the breach may not have sufficient detail to make the decision. To make this decision the essential information is:

- The type and numbers of data subjects affected
- The types of personal data compromised and the number of records

- Initial assessment of the cause of the breach
- The possible consequences of the breach
- Any factors that mitigate the risk from the breached data

The Trust Data Protection Lead will assign appropriate individuals to investigate. This may require additional assistance from the person who discovered the breach.

If possible, information gathered during the investigation should be supported by records, emails, or by reference to other school sources.

At any point in the investigation the Data Protection Lead may decide they have enough information to make the assessment of notification. This does not mean that the investigation is complete, but the decision will determine the timescale for the completion of other activities.

Any documents, notes of meeting, or calls and emails should be recorded on the chronology.

5. Take containment action

Containment means taking action that mitigates the potential consequences of the breach. Providing a breach has been reported quickly, significant mitigation may be possible. In some cases, especially with confidentiality breaches, the time gap between the initial breach and its discovery leaves little room for containment.

There are immediate actions that the person who caused and/or discovered the breach can take, for example:

- recall an email sent in error;
- contact the incorrect recipient to ask them to delete the email and to confirm they have done so;
- request the IT Team to suspend students' email accounts where an email was incorrectly sent to them; or
- deactivate a mobile device.

Before undertaking any more involved action, an assessment must be made to ensure that it doesn't compound the breach – for example by disclosing personal data to additional unauthorised recipients.

If, at this point, criminal activity is suspected (even tangentially, such as the theft of a car containing personal data), the police should be informed, and the crime number should be recorded. If there is strong evidence that a member of the school community has deliberately breached information, then appropriate disciplinary action needs to be initiated.

Even if the actual breach event happened some time before discovery, the questions about whether actions can be taken to mitigate the further spread of breached information should be considered. It can of course be far more difficult to achieve in these circumstances.

Whatever decisions and actions are taken should be recorded in the breach log.

6. Assess the level of notification required

This is a decision that must involve the Trust Data Protection Lead. The guidance of the Data Protection Officer should be sought, although the Trust Data Protection Lead is free to make decisions based on more than the data protection issues.

There are no simple threshold numbers that can be used. Highly confidential information about a small number of people could have very significant impacts on them or other people, while relatively benign data about many people may have little risk to their rights and freedoms.

Each case must be decided upon its specific circumstances. The Data Protection Officer, in fulfilling their role, may decide that the ICO must be alerted to even though the Data Protection Lead has decided not to report an incident.

The rationale for the decision about reporting should be recorded and kept with other details of the breach. If a judgement is made that the ICO must be notified, then it is likely that further investigation will be required before the report can be completed. This means that this decision about notification really needs to come well before the 72-hour window closes.

7. Notification of the breach (where required)

This task, unless there are exceptional circumstances, will be carried out by the Data Protection Officer. Part of the role is to be the interface between the data controller and the regulator. The critical requirement is for the investigation to have been completed and any potential action to contain the breach needs to be in progress or planned.

The Trust Data Protection Lead will need to be available to answer any questions that the ICO may have and to take actions that are recommended.

If notification to the ICO is not required, then the information about the breach in the chronology will be completed and the entry in the breach log will be closed. The same basic information that would go into the ICO notification should go into the local breach log. For local logging the 72-hour timescale is not enforced.

8. Repair the causes of the breach

For organisations to be fully UK GDPR compliant they need to be able to demonstrate that they have engineered data protection by default and by design into their operations. One element of that is to look for continuous improvement in the data protection regime.

Any incident that has been recorded on the breach log should be subject to review. The review team would certainly include the Data Protection Lead but may also include other senior colleagues.

Reviews of specific incidents should be recorded such that they can be filed with the records of the incident.

It may be that the review of an individual case identifies weaknesses in the data protection regime and the team should certainly go on to consider how these weaknesses can be addressed. The review team should also bear in mind that sometimes there is a pattern of incidents (for example

a skew in the distribution of days of the week that incidents occur). These patterns may reveal something systemic in the organisation that needs to be addressed.

If there have been significant breaches, then the review team can consider whether a Data Protection Impact Assessment (DPIA) would be useful to identify specific weaknesses in the processing of personal data in the area of the breach.

Minutes and actions of the review team meeting should be kept and retained for the current year and two years afterwards.

9. Possible indications of personal data breaches (not exhaustive)

The items described in this section form a very small subset of the signs that a breach has occurred. It is essential to remember that there is no requirement to know that the rights and freedoms of individuals have been infringed to recognise that a breach has occurred. It is enough that the infringement could happen.

Consider the three types of personal data breaches – confidentiality, availability and integrity. Many real-world situations combine categories.

For example: A missing paper file of SEND information means that an expected assessment cannot be carried out. When the file is retrieved by the member of staff who took it home, it is discovered that some of the information has been out of date for 18 months. This is the combination of an availability and an integrity breach.

Confidentiality Breaches

Here we are concerned about information falling into the hands of people unauthorised to have it. Obvious cases would be:

- Loss or theft of a computer, tablet or phone containing, or with access to, personal data.
- Loss or theft of a personal bag containing paper records of personal data.
- An individual having access to, or a copy of, personal data not required for their role (note here that, if the person has a role requiring them to produce and manage personal data even though they are not involved in the process that uses the data, this is not a breach).
- Sending an email to the wrong location.
- Disclosing the identity of recipients of an email, when those recipients might otherwise reasonably expect confidentiality.
- Passing on information about a data subject from an individual who is entitled to know to one who is not entitled.

In some cases, it would be relatively easy to identify that the breach had occurred, but in others the initial indications of the breach may be quite diffuse. For example, staff may discover a case of intimidation or bullying and then recognise that it has been based on personal data which might have been obtained in an inappropriate fashion.

In extreme cases the first indication of a breach is the lodging of a complaint with the Trust or the appearance of stories in the traditional media or in social media spaces.

Availability Breaches

An availability breach is probably the easiest to spot because information is not available when it is required.

Possible causes might be:

- A failure of a system like the MIS, HR Database or Visitor Management.
- A file not being returned to its storage location.
- A file being shredded before the end of its retention period.
- Records being erased before their retention period.
- Theft, fire or vandalism.

There are thresholds to consider in the case of an availability breach. If a system is down for a short period of time, or missing for a short period, then this would almost certainly not meet the threshold. The question is whether the lack of availability could have an impact on the rights and freedoms of the data subjects that the information related to.

Integrity Breaches

Integrity breaches occur when personal data is inaccurate. There are two major ways that this occurs:

- Data is captured inaccurately.
- The data becomes out of date.

The breach only appears at the time the data is being retrieved or used and the potential impact of the breach can be highly variable.