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 General Data Protection Regulation (GDPR) with some specific amendments. Section 2 of Chapter IV of the 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.

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.

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 can't be met.

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

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 Comm ű ' sr t %

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 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 Trust and school Data Protection Leads.

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.

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.

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 an(as )-912(eache0000

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.

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.

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 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.