Data Breach Policy

PURPOSE

The Academy 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 (UK 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.

Date of last review:	April 2024	Author:	Data Protection Officer
Date of next review:	April 2027	Owner:	Director of Governance
Type of policy:	☒ Network-wide ☐ Tailored by school	Approval:	Management Team
School:	N/A	Key Contact Name:	Governance team
Key Contact Email:	governance.team@arkonline.org	Key Contact Phone:	020 3116 6333

POSITIONING WITHIN ARK OPERATIONAL MODEL

Component	Element
☐ Strategic Leadership & Planning ☒ Monitoring, Reporting & Data ☒ Governance & Accountabilities ☐ Teaching & Learning ☐ Curriculum & Assessment ☐ Culture, Ethos & Wellbeing ☐ Pathways & Enrichment ☐ Parents & Community ☐ Finance, IT & Estates ☐ Our People	Data Protection

Contents

Introduction

The UK GDPR describes the responsibilities that organisations have when dealing with personal data and at Ark we are committed to our obligations under the UK GDPR to maintain a robust and structured programme for compliance adherence and monitoring.

The sixth principle of the Act 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.*'

Despite the measures we put in place, it is inevitable that accidents sometimes happen which can lead to a personal data breach. In the event of a data breach, there are a set of key actions which must be undertaken which has been explained in this policy. This policy applies to all employees of Trust, governors and/or Trustees, volunteers and a should be read in conjunction with Ark's Data Protection Policy.

This policy will be reviewed every three years, or when the Information Commissioner's Office (ICO) issues revised guidance on this topic.

What is a Data Breach?

A data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

A personal data breach may mean that someone outside the school gets unauthorised access to personal data along with more sensitive types of information like medical or SEN information. Other examples of a personal data breach could be where there is unauthorised access within the school for example an employee accidentally or deliberately changing or deleting personal data.

A data breach occurs if at any point there is any one of the following that occurs:

- A breach of **confidentiality** of personal information
- A breach of **integrity** of the data
- A loss of **availability** of any personal information

This means that a personal data breach is more than just losing personal data and according to the ICO organisations which process (use or store) personal data must take appropriate measures against unauthorised or unlawful processing, accidental loss, destruction of or damage to the personal data we hold and are responsible for.

A personal data breach can happen in a number of ways for various reasons for example:

- Loss or theft of data or equipment which holds personal data e.g., laptops, tablets, removeable drives or paper copies
- Equipment failure
- Inappropriate access controls allowing unauthorised use
- Human error (such as sending an email to the wrong recipient)
- Hacking, phishing, or blagging (information obtained by deception)
- Unforeseen incidents such as fire or flood.

Human error is the most common cause of data breaches and can happen for many reasons:

- Theft or loss of paperwork
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact personal/sensitive data

What is a near miss?

A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out to those within the network only and can be recovered quickly or returned.

We record all near misses in order to understand patterns, learn lessons and implement improvements.

Responsibilities

The Trust will:

Ensure to put in place a clear procedure for handling data breaches. This procedure can be found in Annex 1 and should take account of the requirements on staff.

We will follow any and all guidance published by the Information Commissioner's Office (ICO) ensuring that data breaches are dealt with in line with the statutory time limits.

Take advice from the Data Protection Officer with regards to the management of data breaches and ensure the Data Protection Officer is informed of all data breaches which have occurred across the network and they have been correctly and appropriately reported and recorded.

The Data Protection Officer will:

Provide guidance and support to the Network in dealing when dealing with any data breach and will act as the main point of contact between the Trust and the Information Commissioner's Office in the event of notification being required.

Ensure the ongoing confidentiality, integrity, availability, and resilience of processing, systems, and services used within the network.

Annex 1: Procedure for managing a Data Breach

Identifying a Data Breach

All members of staff at the Trust have been trained in identifying when a data breach has potentially occurred. Whether the staff member has been involved in the breach themselves or has been informed a breach has occurred (for example by parents, students, or other stakeholder), all breaches must be reported to the relevant data protection staff member without delay.

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 to the school's Data Protection Lead or Ark's Data Protection Officer (DPO) as soon as possible.

If a data breach has occurred within school, please speak in the first instance to the school's Data Protection Lead (DPL), otherwise all data breaches, queries, or concerns can be sent to Ark's DPO using dataprotectoin@arkonline.org, and this includes reporting breaches outside of normal working hours, on the weekends, or outside of term time.

In the case of a personal data breach that must be reported to the ICO, we have 72 hours to inform the ICO of our initial findings. 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 their laptop is stolen, this is the start of the 72-hours not when it is reported to the Trust after the weekend.

Where a data breach is identified the schools designated Data Protection Lead and the DPO must be informed immediately. The Data Protection Lead (with support from the Data Protection Officer) will investigate the occurrence and complete a Data Breach Incident Report form which will help to determine the notification requirements.

Members of staff are not expected to independently investigate or fix any potential breaches before bringing them to the attention of the Data Protection Lead or DPO however, they should act quickly and report the breach the responsible individual.

Information required when reporting a breach:

From the initial report, it is essential to establish the timeline of the breach and at the first stage the person reporting the breach should provide the Data Protection Lead or DPO with:

1. The time and date when the suspected breach occurred
2. A description of the breach including whether it is a breach of confidentiality, availability, or integrity
3. The types of personal data, individuals, and number of records affected
4. How the breach was discovered
5. Details of any individuals they have discussed the potential breach with

If there are emails, minutes of calls or meetings, or any other documents associated with the discovery of the breach, these should be provided to the Data Protection Lead or DPO to help with the investigation of the breach.

Data breaches or near misses may be identified as part of everyday our business. They may be identified by admin staff, parents or pupils or by a third party like the local authority or an MIS provider.

Investigate

When a data breach has been identified then the Data Protection Lead or Data Protection Officer (called the Lead Investigator) will begin a formal investigation into the events that occurred. The Lead Investigator will determine the seriousness of the breach and the risks arising from it, and with the support of the DPO (if not leading the investigation), establish whether the breach has met the threshold of reporting to the ICO.

Any actions to contain and recover the shared data, as well as mitigate any risks to those involved should be taken by the Lead Investigator immediately. The investigation is to ensure that the case is being managed and any improvement actions have been agreed are implemented.

The report from the individual who discovers the breach may not have sufficient detail to make the decision, therefore the Lead Investigator should identify:

- Whose data was shared in the breach
- What type of data and number of records involved
- How it happened
- The potential impact on those whose data was shared (also known as Data Subjects)
- What immediate steps are required to remedy the breach
- What lessons can be learnt to avoid a recurrence

The Lead Investigator may assign an appropriate staff member to undertake the investigation and may require additional assistance from the person who discovered the breach in order to contain and remedy the incident.

Whenever a breach occurs, a Data Breach Incident Report form should be completed by the Lead Investigator. This form is an essential part of the reporting process and should include:

- The type of data shared and its sensitivity
- How many individuals are affected by the breach and the potential impact on them (for example could the data be used illegally or shared inappropriately i.e., on social media)
- What protections are/ were in place to prevent the breach from happening
- What happened to the data and has it been returned/securely disposed of
- Had the staff member involved in the breach received or taken Data Protection training
- What types and number of people have been affected
- The cause and the risk rating of the breach

The form also includes a chronology of the breach and lists the actions taken by the Trust or school to remedy the incident. If there are any emails, minutes of calls or meetings, or any other documents associated with the breach, these should be recorded within the Data Breach Incident Report form.

Within the form we also include any recommendations of actions, which will be implemented by the school, central team, or the network to prevent a recurrence of the same type of data breach.

An initial Data Breach Incident Report form should be completed urgently and wherever possible within 24 hours of the breach being discovered / reported. A further review of the causes of the breach and recommendations for future improvements can be done during the investigation/ once the breach has been resolved.

Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data breach and taking any action that mitigates the potential consequences of the breach on our data subjects.

In order to contain and remedy a potential or actual data breach, we must quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any lost data and limit the damage to the data subjects impacted by the breach.

The Lead Investigator will be managed and supported by Ark's Data Protection Officer, who must be informed immediately of any data breach occurring within the network in order to monitor and provide advice on actions to be taken on any potential or actual data breach.

The Lead Investigator may also require support to contain and remedy the breach from other staff within Ark or external organisations, depending on the severity of the breach, like:

- Central and school IT teams
- Finance
- Senior Leadership Team (SLT)
- Designated and Deputy Safeguarding Leads
- Admin and operational staff
- The LADO
- The Police

Before undertaking any action, an assessment must be made to understand the severity and the immediate actions which can be taken to remedy the breach, ensuring these actions won't lead to further information sharing, for example by disclosing personal data to additional unauthorised recipients.

If during the investigation criminal activity is suspected (such as the theft of a laptop, or forced entry into a building), the police should be informed, and the crime number should be recorded within the breach incident form and log. If there is strong evidence to suggest that a member of school community has deliberately accessed and breached information, then appropriate disciplinary action will be initiated.

Examples of steps taken to remedy a potential or actual data breach may include:

- Attempting to recover any lost personal data or equipment
- Shutting down or ceasing the use of an IT system
- Communication and advice provided to school staff or the network to prevent further breaches and encourage best practice
- Contacting the Admin teams within school and the central External Relations teams (depending on the severity and scope of the potation or actual breach) so they can be prepared to handle any data subject or press enquiries, or to make any press releases
- The use of back-ups to restore lost, damaged or stolen data

- If bank details have been compromised in the breach, contacting banking providers for advice on preventing fraudulent use
- Where the data breach includes access to entry codes or passwords, these codes will be changed immediately, and the relevant organisations and members of staff made aware, ensuring the new access codes are shared appropriately, securely, and only when necessary.

Providing a breach has been reported quickly, action will and should be taken swiftly in order to try to significantly reduce the impact of the breach on data subjects.

Even if the actual breach event happened some time before discovery, the question about whether actions can be taken to mitigate the further spread of breached information will always be considered. It can of course be far more difficult to achieve in these circumstances, but we will work with those involved to contain the spread and recover the shared personal data.

If you are a parent and your child's school contacts you or you are involved in a breach where someone else's personal data has been shared with you, we ask that you support the school and/or trust with securely disposing this information and you will be provided with information and guidance from the Data Protection Lead or appropriate member of staff on how to do this.

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

Informing and advise those at Risk

Ark understands that we have obligations and a duty to report data breaches in certain instances. The ICO requires us to inform those affected where there is a significant breach of personal and sensitive data and the risk of harm to those individuals is high. All staff are aware of these requirements, and we have strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported to the Data Protection Lead and DPO without undue delay.

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and understandable format. Clearly if there was a high risk of further harm, the school would have an obligation to disclose the breach to each individual affected. However, this has to be balanced against the risk of causing further distress and anxiety to the families by informing them about the breach.

Any notification will include:

- The name and contact details of the relevant people within Ark to contact for more information about the breach
- The likely consequences of the personal data breach, along with specific and clear advice on how you can protect yourselves following the incident
- The measures Ark has taken or intends to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects

Only the Lead Investigator and DPO can decide whether to advise affected individuals of a data breach, and depending on the risk and severity of the breach you will either be informed

by Ark's Data Protection Officer (DPO), the school's Data Protection Lead (DPL), or an appropriate member of the Senior Leadership Team (SLT).

Further advice on whether to inform those individuals impacted by a potential or actual data breach is contained in the ICO Guidance on Assessing Disclosure to Individuals affected by a Data Breach.

Data Breach Log

Reporting a breach makes a positive contribution to the Trust in managing its data protection responsibilities and compliance with relevant legislation. All data breaches, including near misses, are recorded within our Central data breach tracker. All incidents identified following the implementation of this policy will be recorded within the tracker and categorised according to whether it is a data breach, near miss or the breach originated within a third party provider or system.

This data is reviewed and analysed to identify patterns and monitor the implementation of preventative measures ensuring they are impactful and achieve their aim.

The DPO will collate all incidents into a single report that includes trends and lessons learnt which is shared with key stakeholders within the trust every term to highlight the impact of data protection across the network.

Examples of Data Breaches

The scenarios described in this section give an idea 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 breach happened.

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

Where a breach has occurred, it is may involve a breach of more than one of the categories listed above. For example, a missing SEND file means that an expected assessment can't be carried out. When the file was retrieved by staff, it was discovered that some of the information had not been updated for 12 months. This would be a breach of availability and integrity.

Confidentiality Breaches

A breach of confidentiality occurs where unauthorised individuals have access to data.

Examples of a breach of confidentiality would include:

- 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
- Sending an email to the wrong recipient or not bcc'ing recipients when sending mass emails
- Disclosing the identity of recipients of, when those recipients might otherwise reasonably expect confidentiality.

In most cases, it is relatively easy to identify when a breach has occurred, however there are cases where is might not be obvious until the investigation begins. For example, staff may discover a case of nuisance or bullying to discover that it begun as personal data had been obtained inappropriately or maliciously.

Availability Breaches

An availability breach is where data is not available when it's required. Now this does not mean where a system or file is not available for a short period of time, but the question is whether the lack of availability could have an impact on the rights and freedoms of the data subjects involved.

Possible causes might be:

- The failure of an IT system like the school's MIS, HR Database or Visitor Management
- Where files have not been returned to their correct storage location
- Files being shredded before the end of their retention period
- Records being erased before their retention period
- Theft, fire, or vandalism

Integrity Breaches

Integrity breaches occur where we have a record of personal data that is inaccurate and this can happen in two ways:

- The data was captured inaccurately
- The data we hold that is out of date

A breach of integrity will occur at the time the data is being retrieved or used and the potential impact of the breach can vary depending if sharing of the inaccurate data has also occurred.

Please not these lists are not exhaustive but instead give an indication of when a breach has occurred.