Academies Trust

8th Floor, Angel Square,
Manchester, M60 0AG

# Data Breach Procedure (Including Cyber Incidents)

Appendix 2 of the Data Protection Policy

Approved by the Trust Board on 3 October 2024

Applicable from 4 October 2024

This document will be reviewed annually, or more frequently when significant changes are made to the law.

## Contents

# Appendix 2: Data Protection - Personal Data Breach Procedure (including Cyber Incidents)

## A2.1 Introduction

We recognise that a breach of personal data could happen, despite our policies, procedures and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to our academies or to individuals.

This procedure supports our Data Protection Policy. It includes our guidelines for reacting to and handling any actual or suspected breach of personal data, as soon as we become aware of the incident, in line with the UK GDPR, the DPA 2018 and best practice.

## A2.2 Scope and Responsibilities

This policy applies to all instances when it is known or suspected that personal data that we handle has been subject to a breach (see below for breach definition).

All staff are responsible for reading, understanding and complying with this policy.

Our Head of Data Protection provides assistance and further guidance on data breaches.

Each academy has a Data Protection Ambassador responsible for taking the lead on the steps in this procedure once a breach, or suspected breach, has been reported internally, including reporting to the Head of Data Protection.

Any staff member becoming aware of a breach is responsible for immediately reporting it. Please refer to the Breach Response Plan below for the necessary steps to follow.

## A2.3 What is a Personal Data Breach?

If personal data we handle is lost, destroyed, altered, disclosed, accessed or put beyond use when it shouldn't be, this is a Personal Data Breach.

Where we suspect personal data has been subject to a breach, we will follow this procedure until we are sure that the personal data has or hasn't been breached.

A personal data breach can occur accidentally or intentionally, and can be caused by staff, by an external threat (including cyber incidents), or anyone else.

## A2.4 Breach Response Plan

All members of staff are responsible for taking all reasonable steps and cooperating with key staff in following this procedure when a breach is found or suspected (including Cyber incidents/attacks).

The breach response plan has 9 steps, which are covered in detail below:

1. Report the breach internally;
2. Contain;
3. Record the breach (using the GDPRiS software);
4. Investigate and assess the risk;
5. Notify the ICO of the breach (if applicable);
6. Notify the affected Data Subjects of the breach (if applicable);
7. Maintain records;
8. Close and reflect;
9. Implement any necessary changes to prevent reoccurrence.

### A2.4.1 Report the breach internally (All staff)

As soon as staff are aware that a data breach has occurred, they must immediately inform their data protection ambassador or the headteacher in their absence. The data protection ambassador will lead on the breach response, including informing the Head of Data Protection of the breach and keeping them updated on any subsequent investigation or actions.

Should the breach involve data that is held centrally, as opposed to a particular academy, then central team colleagues should alert the Head of Data Protection directly, or in their absence the Data Protection and Information Governance Apprentice.

The report should be made as soon as possible, even if the breach is discovered outside of normal working hours.

### A2.4.2 Contain (All staff with support from Data Protection Ambassador and/or Head of Data Protection)

Once you become aware of a breach you need to act quickly. The first priority is not "do we need to report this to the ICO?" (though this is important and is addressed below). The first priority is to contain the breach. Think of it as a fire - you wouldn't stand around and discuss the implications of it until the fire itself was out.

You should consider the data that has been breached and assess whether there are any actions you can take to stop the breach from getting any worse.

Containment and recovery actions could include, as appropriate:

- Attempting to find lost devices or paperwork;
- If devices have been stolen, reporting this to the police;
- If a breach is still occurring, for example, due to an ongoing IT issue, then IT should take appropriate steps to minimise the breach, such as closing down an IT system or server. In the event of a Cyber attack, immediately report to the Action Fraud line on 0300 1232040.
- Warning staff and third parties such as the County Council, to be aware of any "phishing" attempts that might be linked to personal data that has been accessed by criminals/unauthorised people;
- If data has been sent to, or shared with, someone it shouldn't have been, considering whether you can contact them to recover the data. Bear in mind that "recall" doesn't usually work on externally sent emails; if you have used virtru to encrypt the email before sending it you can revoke the third party's access;
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use;
- If the data breach includes any entry codes or IT system passwords, changing these immediately and inform the relevant agencies and members of staff;
- Contacting the Trust's Brand and Communications Team, so that they can be prepared to handle any press enquiries.

### A2.4.3 Record the breach (Data Protection Ambassador)

All breaches, regardless of how big or how small, must be recorded by the Data Protection Ambassador using the Trust's chosen software, GDPRiS. Data Protection Ambassadors can seek further guidance on how to report a breach in their Data Protection and Information Governance Handbook, but should Include as many details as possible and attach documents or evidence if appropriate.

If full details aren't available immediately, log what information is available, and add more detail as it becomes available.

### A2.4.4 Investigate the breach and assess the risk (Data Protection Ambassador and Head of Data Protection)

Once the immediate controls have been put in place, review how the breach happened, going right down to the root causes of the breach. Consider all possible impacts on the situation that may have caused, or contributed to the breach. Identify what changes will help prevent any similar breaches in future.

Data Protection Ambassadors, with the support of the Head of Data Protection, will be expected to seek answers to the following questions:

- What are the circumstances that led to the breach? What happened? Who was involved? When did the academy become aware that a breach had occurred?
- What data has been breached?
- What data subjects are affected?
- Are any of those data subjects now vulnerable or at risk as a result of the data breach?
- What can we do to reduce the risk to data subjects?
- Who was responsible for the breach?
- Have they had training? If so, when?
- Was their training in the last 2 years?
- What actions can be taken to prevent further breaches from taking place?

Consider what harm could come from the breach, including who could be harmed, how they could be harmed, and how severe the harm could be, as well as how likely it is the harm will happen. This risk assessment, based on severity and likelihood, will depend on the types of information involved (how sensitive is it, what could be done with it?), how much information is involved, and how exposed the data is, as well as the individual circumstances of the data subjects (the person or people the data is about).

As an example, if a laptop has been lost, if it is encrypted there is a very small chance of any data being accessed. But if hard copy documents have been lost or left unattended, they are much more likely to be accessed and read.

As another example, if personal data is included in an email by accident, the data may be at more risk of being misused if the email has gone to a member of the public, rather than to another school.

As an example of the need to assess the data subjects' circumstances, accidentally disclosing an address might not pose a risk to most data subjects, but it could be very high risk for someone who is escaping domestic violence, or for the adoptive family of a child.

### A2.4.5 Notify the Information Commissioner's Office (ICO) of the breach (Head of Data Protection)

The decision about whether to report a breach to the ICO is made by the Head of Data Protection. Breaches that could cause a risk to people should be reported to the Information Commissioner's Office (the ICO – the UK's data protection regulator) and, in some cases, to the data subject(s) involved too.

Not all breaches will need to be reported. For example, if data is deleted in error it is technically a breach, but if the data is backed up and can be promptly reinstated, it does not represent a risk to data subjects.

If the Head of Data Protection decides not to report a breach to the ICO and/or the data subjects involved, the decision and reasons will be recorded.

If it is likely the breach will result in a risk to people's rights and freedoms, it must be reported to the ICO.

Reports to the ICO must be made within 72 hours of us becoming aware of the breach. Information can be provided to the ICO in stages, giving them the details as and when we find out more, but the first contact must be within 72 hours.

The ICO will want to know the following information:

- A description of the personal data breach that has occurred including, where possible:
    - The types and approximate number of people whose data is involved;
    - The types and approximate number of personal data records involved;
- The likely consequences of the breach;
- The measures taken, or proposed to be taken, in response to the breach, including actions to mitigate any possible harm to data subjects;
- The name and contact details of the Head of Data Protection, or any other contact details of people who can provide more information.

Guidance on how to report to the ICO is on their website:
https://ico.org.uk/for-organisations/report-a-breach/

### A2.4.6 Notify the affected Data Subjects of the breach (Head of Data Protection)

If the risk to data subjects is assessed as high, the breach must also be reported to everyone whose data is involved, to allow them to take any appropriate steps to protect themselves and so they are aware of anything that may happen. For example, if financial information has been lost or stolen, they can alert their bank for fraudulent activity, or if passwords have been lost or stolen they can change them on their accounts and any other accounts that they used the same password on.

We can choose to report to data subjects even if the risk is not high, if it would be better for us to tell them about the breach for other reasons, such as supporting transparent relations and trust.

In many circumstances it will be preferable for data subjects to hear about a breach from us rather than from any other source.

### A2.4.7 Maintaining records

Ambassadors and the Head of Data Protection will keep an accurate record of all events that occur throughout the course of an investigation, through to the completion of the incident. Such records will be maintained on GDPRiS and may be provided to the Information Commissioner's Office upon request.

### A2.4.8 Reflect and Close

At the conclusion of the incident, the Ambassador should ensure that the record on GDPRiS is up to date and that the record is closed appropriately. Further guidance on how to do this is available in the Data Protection and Information Governance Handbook contained in the toolkit.

It's always useful to have a period of reflection. Ambassadors should include the Senior Management Team in such reflections and consider whether any lessons could be learned from the breach. Do your data protection practices need to change? Can any further support or training be offered to staff? Consider how effective the response was, and if improvements could be made when handling any future breaches.

As examples, did the person who first became aware of the breach know to report it internally? Did attempts to recover the data work? How could the breach have been handled better or quicker?

The Senior Management Team should consider whether any systemic or ongoing problems are identified, and ensure an action plan is drawn up to put these right. If the breach warrants a disciplinary investigation, senior management will liaise with Human Resources for advice and guidance.

### A2.4.9 Implement any necessary changes to prevent reoccurrence

Depending on what the review indicates about how the breach occurred, actions should be taken to reduce the risk of something similar happening again, including amongst other things, improved IT security, new or improved written procedures, refresher training, improved supervision, changes to processes, communications to remind colleagues about risks, etc.