Personal Data Breach Policy and Procedure

Document title	Personal Data Breach Policy and Procedure		
Owner	Compliance		
Version	1	Status	Final
Last updated	04.03.2024	Last updated by	Lea Millinchip - Compliance Officer
Approved on	01.06.2024	Effective from	01.06.2024
Review Date	01.06.2026		
Purpose	To be used following an actual or suspected personal data breach		
This policy links to:	GDPR		

If you would like this information in another language or format, please speak to the Trust HR Operations team.

Phone: 01543 622433

Email: lea.millinchip@stchads.uk

1.0 Introduction

1.1 This policy and procedure is to be used by the Trust's Data Breach Response Committee if there has been a personal data breach (or a suspected personal data breach). The Committee is comprised of the senior members of staff (named at section 0 below) who will deal with different aspects of the personal data breach.

1.2 All staff receive training on how to recognise a personal data breach and the Trust's Information Security Policy contains guidance for staff on this issue.

1.3 The Trust is required to report certain breaches to the Information Commissioner's Office (**ICO**) and to data subjects under the UK GDPR. There are strict timescales for reporting breaches which are outlined in section 0.

1.4 The Trust also has responsibilities to report certain incidents to other regulators such as the Education and Skills Funding Agency. Section 0 also covers these reporting obligations.

1.5 Immediate action following a personal data breach

- Inform all members of the Data Breach Response Committee.
- Identify what personal data is at risk.
- Take measures to prevent the breach from worsening e.g. changing password / access codes, segregating the information held on the Trust's systems.
- Recover any of the compromised personal data e.g. use back-ups to restore data.
- Consider whether outside agencies need to be informed as a matter of urgency e.g. the police if there has been a burglary, or Children's Services where the breach may lead to harm being caused to a pupil.
- Consider whether any affected individuals should be told about the breach straightaway. For example, so that they may take action to protect themselves or because they would find out about the breach from another source. Please note this is different to the mandatory notification to individuals covered at 7.1 - 7.7 below which does not need to be an immediate notification.
- In the vast majority of cases, notify insurers without delay.

2.0 What is a personal data breach?

2.1 A personal 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.

2.2 If staff are in any doubt as to whether an incident constitutes a personal data breach, they must speak to the Data Protection Officer] immediately.

2.3 Please see Appendix 1 for examples of personal data breaches.

3.0 Roles and responsibilities

3.1 The following staff form the Trust's Data Breach Response Committee (the **Committee**) and will have certain responsibilities:

Role	Responsibility
The Data Protection Officer	The Data Protection Officer will chair the Committee and is responsible for co-ordinating the Trust's response to any breach.
The Director of Operations	The Director of Operations will lead on any physical security measures which are required at the Trust site to contain the breach. The Director of Operations is responsible for notifying and liaising with the Trust's insurers as required.
The Principal	The principal will be responsible for any communications with pupils and parents and for any pupil welfare or disciplinary considerations.
The HR Officer	The HR Officer will lead on any employee welfare or disciplinary issues in consultation with the Principal.
The Data Protection Officer	The Data protection Officer will be responsible for ensuring the security of the Trust's ICT infrastructure. In addition, for taking any possible technical measures to recover personal data or to contain a personal data breach.
The Chief Executive Officer	The Chief Executive Officer will be responsible for liaising with the Board of Trustees as appropriate. Any decision to report the personal data breach to the Education and Skills Funding Agency will be taken by the Board of Trustees.

3.2 The Committee will form as soon as possible once a personal data breach has been identified.

4.0 Containment and recovery

4.1 As soon as a personal data breach has been identified or is suspected, steps will be taken to recover any personal data and to contain the breach. For example, the Trust will consider the need to:

- Change any passwords and access codes which may have been compromised.
- If appropriate in all the circumstances, tell employees to notify their bank if financial information has been lost (or other information which could lead to identity theft or financial fraud) and consider offering credit protection.
- Limit staff and / or pupil access to certain areas of the Trust's IT network.
- Use back-ups to restore lost or damaged data.

- Take any measures to recover physical assets e.g., notifying the police or contacting third parties who may have found the property.
- Notify insurers; and
- Take action to mitigate any loss.

4.2 Where appropriate the Committee will delegate tasks to other members of staff with the relevant expertise.

4.3 The Committee will seek assistance from outside experts, if appropriate, to effectively contain the breach and recover any personal data. For example, legal advice, reputation management advice or specialist technical advice.

4.4 If the breach concerns a cyber or IT related issue, then the Trust will consider whether it would be appropriate to involve external IT experts to assess the extent of the breach, to advise on remedial steps and to verify that remedial steps taken by the Trust are sufficient to remove the risk of a further breach. Guidance from the National Cyber Security Centre (National Cyber Security Centre - NCSC.GOV.UK) will be followed if this is considered appropriate by the Trust's Data Protection Officer.

4.5 The Trust will ask its insurers how much they want to be involved in the Trust's response. The insurers might provide access to additional resources and expertise, such as forensic IT experts.

4.6 The Trust will run any correspondence past its insurers for approval before sending out (for example, letters notifying affected data subjects of the breach). However, the Trust will act as a reasonably prudent uninsured, this means that the Trust will not delay taking action if insurers are slow to respond and a delay would prejudice the Trust's position.

4.7 The Trust's insurers will be kept updated in relation to new developments and progress.

5.0 Establishing and assessing the risks

5.1 To assist with this process, the Committee will document the answers to the questions contained in Appendix 2 in as much detail as possible.

5.2 The table in **Error! Reference source not found.** will be copied into a new document in order to retain a record of this process.

5.3 The Trust will also consider whether there are any safeguarding considerations. For example, if the breach may lead to a pupil being put at risk of harm. If so, the Trust's safeguarding policy will be followed.

6.0 Notification

Notification to the Information Commissioner's Office

6.1 The Trust is required to report a personal data breach to the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The process described in section 0 above will be used to determine if a notification to the ICO is required.

6.2 Any decision to not notify the ICO will be documented. If another personal data breach occurs in the future the ICO might ask why any previous breaches were not reported and the ICO may ask to see evidence of any decision to not notify.

6.3 If the Trust decides to notify the ICO then this will be done without undue delay and within 72 hours of having become aware of the breach.

6.4 Content of the notification

6.5 The ICO has set out procedures for notifications on its website (ico.org.uk) which will be followed.

6.6 The initial notification within the 72-hour period will contain as a minimum:

- A description of the nature of the personal data breach including where possible:
- The categories and approximate number of data subjects concerned; and
- The categories and approximate number of personal data records concerned.
- The name and contact details of the Data Protection Officer who can provide more information to the ICO if required.
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken or proposed to be taken by the Trust to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. The Trust will include here any follow up measures that will be taken, such as additional training, or updating of policies and procedures.

6.7 In so far as it is not possible to provide all of the information above within 72 hours, the Trust will provide it later so long as there has been no undue delay.

6.8 If it has not been possible to submit the notification to the ICO within 72 hours of becoming aware of the breach, the notification will explain the reason for this delay.

6.9 Even if the Trust is able to provide all of the information in section 6.6 above within 72 hours, the Trust will consider whether it would be beneficial to provide an update to the ICO once more information is known.

6.10 For example, additional information that might count in mitigation. For this reason, the follow up report is an important document as it is the Trust's opportunity to set out to the ICO everything the Trust wants the ICO to take into account in mitigation.

6.11 Where appropriate, the ICO will be told about the measures the Trust already had in place before the breach occurred, as well as the steps the Trust has taken to prevent a reoccurrence.

6.12 The Trust notes that the ICO is less likely to take enforcement action if it considers that there were already robust measures in place and / or the Trust has taken steps to address what went wrong.

7.0 Contacting affected individuals

7.1 The Trust must by law report a personal data breach to the individuals whose data has been compromised (known as data subjects) where the breach is likely to result in a high risk to the rights and freedoms of individuals.

7.2 The process in section 0 above will also assist with any decision to notify data subjects. A notification does not need to be made where:

- The Trust had taken measures so that the data compromised was unintelligible to any person not authorised to access it (e.g. it was successfully encrypted); or
- the Trust has managed to contain the breach or take mitigating action so that any high risk to individuals is no longer likely to materialise (e.g. an unencrypted memory stick has been recovered before anyone was able to access the data held on it).

7.3 If the Trust decides not to notify individuals this decision will be documented.

7.4 If a notification is required then this will be done without undue delay. However, the Trust will also have regard to the wider context and sometimes it is appropriate to delay notification. For example:

- It may not be appropriate to announce that the Trust has been the victim of a cyber-attack until the Trust's systems are secure again; and
- The Trust may wish to consult with social services regarding the timing and content of any notification, for example, where the breach concerns vulnerable individuals.

7.5 The ICO may advise or require the Trust to notify individuals. The Trust will follow the ICO's advice unless there are exceptional reasons not to.

7.6 If a personal data breach relates to children, sometimes it will be appropriate to notify the parents or guardians instead of, or in addition to, the pupils.

7.7 In some cases it will be appropriate to consult with third parties before making a notification to affected data subjects or to other individuals. For example, discussing with the police first if a notification could prejudice a police investigation (e.g. tipping off risks) or discussing with Children's Services if a notification could result in a safeguarding risk.

8.0 Content of the notification to individuals

8.1 The notification to individuals will include the following as a minimum:

- The nature of the personal data breach.
- The name and contact details of a person at the Trust who can provide more information. The Committee will choose the appropriate staff member at the Trust, which is likely to depend upon which individuals are affected.
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken or proposed to be taken by the Trust to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.2 In addition, the Trust will consider if any additional information would be helpful to data subjects. For example, instructions on measures which they can take to protect their data now or in the future.

8.3 The notification will be drafted in clear language. If directed at pupils the notification will be age appropriate.

8.4 The Committee will decide what is the most appropriate method of communication for the notification. Factors to consider include the urgency of the notification. For example, it may be appropriate to telephone individuals and follow up by email.

9.0 Serious Incident Report to the Education and Skills Funding Agency

9.1 An academy trust's funding agreement makes it clear that the Charity Commission's guidance on serious incident reporting must be followed by academies and, accordingly, that serious incidents should be reported to the Education and Skills Funding Agency, as the principal regulator of academies, as soon as reasonably possible after the incident has happened or immediately when the academy trust becomes aware of it. Where there has been a personal data breach, the Trustees will need to consider whether to make a serious incident report to the Education and Skills Funding Agency.

9.2 Trustees should consider the Charity Commission's guidance on reporting serious incidents and in particular, the examples of what to report in the "Data breaches or loss" section in their table of examples.

9.3 The Education and Skills Funding Agency has extensive information sharing powers with other regulators, like the ICO, so the Education and Skills Funding Agency may be aware if a serious incident report is not made. This does not absolve the trustees of the obligation to make a serious incident report, rather it increases the likelihood of the Education and Skills Funding Agency detecting a failure to do so.

9.4 The Trust should make reference to the whole of the guidance and examples table. The examples table gives a data breach reported to the ICO as an example of an incident to report. Because of the breadth of the Charity Commission's criteria for making serious incident reports, trustees should consider whether to make a report in light of the personal data breach and surrounding circumstances - even where it has not been necessary to notify the ICO.

10.0 Notification to the police

10.1 The Trust will consider whether the police need to be notified about the personal data breach if it is possible that a criminal offence has been committed. However, the Trust will not always do this because there is no legal obligation to notify the police. The following are examples of breaches where a criminal offence may have been committed:

- Theft e.g., if a laptop has been stolen.
- Burglary.
- If a staff member has shared or accessed personal data where this was not required as part of their professional duties e.g. a staff member shares information about a pupil with famous parents with the local press; or
- The Trust's computer network has been hacked (e.g. by a pupil or a third party).

10.2 Action Fraud is the national fraud and cybercrime reporting centre. It can be contacted on 0300 123 2040 or using www.actionfraud.police.uk

11.0 Notification to the National Cyber Security Centre (NCSC)

11.1 If the breach relates to a cyber security incident, then the Trust will also consider reporting to the NCSC. There is no legal obligation to do this but the NCSC can provide information and guidance to support the Trust in its response.

11.2 Other regulators, such as the Education and Skills Funding Agency and the ICO may ask if the breach has been reported to the NCSC.

12.0 Other notification

12.1 The Trust will also consider if any further notification is appropriate in the circumstances. For example, if passport information has been compromised, whether a notification to the passport office is appropriate.

13.0 Internal Breach Register

13.1 The Trust is required to keep a register of all personal data breaches including those that do not meet the threshold to be reported. Staff will be trained to report all personal data breaches to allow the Trust to meet this requirement. The Information Security Policy contains further guidance for staff on this point.

13.2 The Data Protection Officer is responsible for keeping this register up to date.

14.0 Evaluation of the Trust's security measures

14.1 The Trust is obliged under the UK GDPR to implement technical and organisational measures to protect personal data. The Trust regularly evaluates the effectiveness of both its technical and organisational measures.

14.2 Organisational measures include:

- Policies for staff on their data protection obligations, including when working away from the Trust site.
- Guidance for staff on how to use specific computer applications and software securely; and
- Data protection training for staff.

14.3 Technical measures include:

- The use of encryption.
- Limiting access to certain areas of the Trust's IT network.
- Firewalls and virus protection; and
- The use of backups.

14.4 The Committee will establish how the existing measures could be strengthened and what additional measures should be put in place to guard against future personal data breaches. The Committee will consider both breaches of a similar type to that which has occurred and the risk of breaches more broadly.

14.5 The Committee may delegate this task to one or more appropriate members of staff. The Committee will consider whether legal and / or technical advice is required. This includes whether it would be appropriate to include external advice from IT experts.

14.6 This exercise will be undertaken promptly because the actions taken by the Trust to improve its practices will likely be taken into account by the ICO when considering if enforcement action should be taken against the Trust.

14.7 Key points to consider include:

- Would improvements in the training given to staff have prevented the breach or lessened the severity of the breach?
- Can measures be taken to speed up the process of staff reporting breaches?
- Does the Trust's Information Security Policy need to be revised?
- Are changes required to the Trust's IT system?
- Should the Trust's document management system be made more robust? For example, should staff's ability to access certain documents be limited to a greater extent?
- Does the physical security of the Trust, particularly in areas where personal data is kept, need to be improved?
- Do the Trust's remote working practices need to change?
- Does the Trust need more robust procedures around staff using their own devices for Trust work?
- Do the Trust's contracts with processors (e.g. a Cloud storage provider) need to be revised?
- Does the Trust need to do more robust due diligence on its processors?
- If any IT services providers were contracted by the Trust to carry out work related to information security was the service provided adequate?

14.8 The Committee will analyse the Data Breach Register at regular intervals so that any trends can be picked up and the relevant measures strengthened.

14.9 The Committee will report the outcome of the evaluation to the Board of Trustees before implementing any necessary changes.

15.0 Evaluation of the Trust's response to the personal data breach

15.1 When the immediate action has been taken following the personal data breach, the Trust will evaluate how its initial response to the breach could have been better.

15.2 Key points to consider:

- Was the breach reported to the Data Protection Officer immediately? If not, what action can be taken to speed up the process of contacting a senior member of staff.
- Were all possible measures taken to recover the data promptly?

- Could more have been done to contain the breach as quickly as possible?

- If one of the Trust's processors (e.g. a payroll supplier) was either responsible for the breach, or discovered the breach, was this notified to the Trust without undue delay? If not, what measures can be put in place to improve this communication in the future?

15.3 The Committee will report the outcome of the evaluation to the Board of Trustees before implementing any necessary changes.

16.0 Other considerations

16.1 The Trust will refer to Appendix 4 which outlines tactical and supplemental considerations. For example, is any pupil disciplinary action required?

17.0 Monitoring and review

17.1 The Data Protection Officer will ensure that this policy is regularly reviewed and updated as required.

17.2 This policy will be reviewed following any personal data breach at the Trust which meets the threshold to be reported to the ICO.

Appendix 1 Examples of personal data breaches and the next steps

Example of breach	Containment and recovery	Establishing and assessing the risks	Notification	Evaluation of the Trust's response to the personal data breach
A staff member leaves papers containing information about pupils' academic performance, including detailed information about where each pupil can improve, on a bus whilst travelling to school. The papers were not in a locked case.	The Trust should find out if it is possible to retrieve the papers. For example, by calling the bus company's lost property department.	The Trust should work through the questions in Appendix 2 below.	If the papers are not retrieved then this breach will need to be notified to the ICO. Whether a notification to the pupils and their parents is required will depend upon the nature of the personal data and the age of the pupils. The Trust should consult section 0 of this policy.	The Trust should work through section 4.0 of the policy above.
Ransomware locks electronic files containing personal data.	The Trust should have a back-up of the data and should also ensure that its systems are secured (e.g. that the ransomware has been removed).	The Trust should work through the questions in Appendix 2 below.	Depends on factors such as whether the Trust was able to recover the data, whether the Trust can be satisfied that the data was not viewed or exfiltrated and whether there is any other risk to the Trust's systems or to personal data.	The Trust should work through section 4.0 of the policy above.
Sending an email containing personal data to the incorrect recipient.	Consider using the recall email feature if available, although sometimes this may not be advisable as it may just draw attention to the email that was	The Trust should work through the questions in Appendix 2 below.	Depends on the sensitivity of any personal data contained in the email, the identity of the unintended recipient, whether the unintended recipient has	The Trust should work through sections 4.0 of the policy above.

	sent in error. Consider also calling the unintended recipient and asking them to delete the email and confirm in writing that they have done so without reading the contents.		agreed to delete it etc.	

Appendix 2 Establishing and assessing the risks presented by the personal data breach

	Question	Response
1	Precisely what personal data has been (or is thought to have been) lost, damaged or compromised, become unavailable or had its integrity compromised?	
2	Is any of the data Critical Trust Personal Data as defined in the Trust's [• Data Protection Policy: Practical Guidance for Staff and Information Security Policy]? This would be information about: • child protection or safeguarding matters. • someone's special educational needs. • a serious allegation made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved). • financial information (for example, a parent's bank details or a staff member's salary). • an individual's racial or ethnic origin. • an individual's political opinions. • someone's religious or philosophical beliefs. • trade union membership. • someone's physical or mental health. This includes information about the provision of health care which reveals information about their health status. • sex life or sexual orientation.	

	• genetic information. • actual or alleged criminal activity or the absence of criminal convictions (e.g. Disclosure and Barring Service checks); and • biometric information used for the purpose of uniquely identifying an individual (e.g. fingerprints used for controlling access to a building). If any of these types of data are involved this makes the breach more serious.	
3	Who are the affected individuals e.g. staff, parents, pupils, third parties?	
4	How many individuals have likely been affected and how many potentially affected in a worst-case scenario?	
5	What harm might be caused to individuals (not to the Trust)? The individuals do not necessarily need to be those whose personal data was involved in the breach. Harm should be interpreted broadly, for example to include: • distress. • discrimination. • loss of confidentiality. • financial damage. • identity theft. • physical harm; and	

	• reputational damage.	
6	What harm might be caused to the Trust? For example, reputational damage and financial loss.	
7	What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point: • Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost / stolen? • Were any technical protections in place e.g. was the data protected by encryption? • Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised? • Have measures been taken to recover the data e.g. has lost data been found before being seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged? • Was the breach a result of actions which were in breach of the Trust's policies?	

Appendix 3

Legal advice

The Trust will consider taking legal advice in relation to the following. This is not an exhaustive list but should be used as a guide.

1 Determining whether to notify the ICO and the data subjects.

2 Drafting the notification to the ICO and the data subjects.

3 Drafting a serious incident report to the Education and Skills Funding Agency.

4 Any correspondence with other external agencies such as Ofsted or the Department for Education.

5 Any communications with the police.

6 The decision to notify the Trust's insurers.

7 Any communications with staff members, pupils and parents.

8 Any disciplinary action in relation to pupils or staff.

9 Establishing whether there is a risk that an affected individual might bring a legal claim against the Trust.

Reputation management

The Trust will consider obtaining advice regarding reputation management. As above, this is not an exhaustive list but should be used as a guide.

The following circumstances in particular may require specialist advice:

1 If the personal data breach becomes widely known to the parental community.

2 If news of the breach becomes known outside of the Trust community.

3 If the media report on the breach or ask the Trust for a statement.

4 If the ICO takes enforcement action which may become public knowledge.

The Trust will consider preparing draft communications in advance, rather than waiting until the Trust is contacted.

Appendix 4 Other considerations

This appendix will be completed as required when a data breach occurs to assist the Trust in checking that all issues surrounding the personal data breach have been considered. It is not an exhaustive list but may assist the Committee when handling the consequences of the personal data breach.

Supplemental issue	**Considerations**
Pupil welfare	
Staff welfare	
Parental complaints	
Staff disciplinary action	
Pupil disciplinary action	
Reputation management	
Risks of legal claims	
Possible Education and Skills Funding Agency action	
Contractual issues	