Growth Academy Trust

Data Breach Procedure Policy

Policy date: October 2022
Review date: October 2023

1. Purpose and scope

1.1 The purpose of this procedure is to provide a framework within which the Trust will ensure compliance with the legislative requirements of managing a **personal data** breach incident, or suspected personal data breach incident.

1.2 This procedure applies to Trust Staff, School staff, agency workers, student ambassadors, volunteers, contractors third party agents and data processors who process data for or on behalf of the Trust and it must be complied with in the event of a personal data breach.

1.3 The Trust is required to keep a record of all security incidents involving personal data. Some of these incidents must be reported to the Information Commissioner within 72 hours of detection, and without undue delay to individuals affected by the incident. It is vital that all staff report a personal data breach, or suspected personal data breach, however minor, as soon as possible after discovery to the Data Protection Officer in order for them to use the 72 hours to establish what has happened, the size of the breach and whether it needs to be reported further.

2. Personal data breach

2.1 A personal data breach can be broadly defined as a security incident that has affected the **confidentiality**, **integrity** or **availability** of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

2.2 Examples of personal data breaches:

- Loss or theft of personal data or equipment (encrypted and non-encrypted devices) on which personal data is stored, e.g. loss of paper record, laptop, iPad or USB stick
- Inappropriate access controls allowing unauthorised use, e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to personal data or information systems
- Equipment failure or significant disruption to normal service (not a maintenance check)
- Human error, e.g. email containing personal data sent to the incorrect recipient
- Unauthorised disclosure of sensitive or confidential information, e.g. document posted to an incorrect address or addressee
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- Insecure disposal of paperwork containing personal data

3. Why should breaches be reported?

3.1 The longer an incident goes unreported, the harder it gets to resolve any vulnerabilities. Impacted data subjects may have a right to know that their data may have been compromised where there is a high risk to their rights and freedoms and that they should take steps that could minimise an adverse impact on them, such as informing their bank that their bank details have been compromised.

3.2 The longer an incident goes unreported, the longer a vulnerability may remain unaddressed, allowing the incident to escalate or for further incidents to occur. Without timely visibility of the incident through reporting the Trust may not be able to fulfil its legal obligations.

3.3 Knowing that a breach has occurred and delaying reporting reduces the time available for the DPO to understand and assist with a response and still meet privacy compliance requirements.

3.4 Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust to prevent future breaches and protect personal data.

4. What to do in the event of a breach

4.1 On finding or causing a breach, or potential breach, the staff member must immediately notify the senior leadership team and the Trust's Data Protection Lead who shall, in turn, immediately inform the DPO. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

4.2 The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach and recovering any personal data. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

- remote deactivation of mobile devices;
- shutting down IT systems;
- recalling an email where possible;
- contacting individuals to whom the information has been disclosed and asking them to delete the information; and
- recovering lost data.

4.3 When the Trust has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

4.4 Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

- what data/systems were accessed;
- how the access occurred;
- how to fix vulnerabilities in the compromised processes or systems;
- how to address failings in controls or processes.

4.5 Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why and reviewing policies and procedures.

4.6 The Data Protection Lead or relevant person should fill in the Data Breach Reporting Form (see annex 2) to be as fully informed as possible and send this to the DPO. The breach spreadsheet should be updated as and when updates come in. All relevant information surrounding the breach should be handed to the DPO, including but not limited to Data Protection Impact Assessments, the data mapping spreadsheet and contracts relating to relevant processors or data sharing agreements for joint controllers. The DPO may decide to take further investigative measures depending on the severity of the breach situation and the Trust's point of contact should be prepared to keep the DPO updated during this breach period.

4.7 Initially the information that need to be provided to the DPO should include the following:

- The nature of the personal data breach including the categories and number of data subjects concerned, alongside the categories and approximate number of personal records concerned.
- The likely consequences of the data breach
- The measures existing and proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Further questions asked in the template.

4.8 The DPO will alert the Data Protection Lead if this has not already been done; the Data Protection Lead should inform the chair of Trustees using the completed Data Breach Reporting Form.

4.9 The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members and/or data processors where necessary.

4.10 The DPO will assess the potential consequences, based on how seriousness, and how likely they are to happen, based on an evaluation of the information in the Data Breach Reporting Form and discussions with the Trust's Data Protection Lead. There will be particular attention on the likely risks to rights and freedoms of the individual (s) affected by the breach.

4.11 The DPO will assess whether the breach must be reported to the ICO based on the adverse effects, risks to rights and freedoms of the individuals, and likely consequences of the breach. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

4.12 If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the Trust who will ultimately decide whether the DPO should report the personal data breach to the ICO.

4.13 The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored both with the DPO on a computer system and with the Data Protection Lead within the Trust. The DPO's advice is written on the Breach Reporting Form and sent back to the Data Protection Lead.

4.14 The Trust board, Data Protection Lead and DPO will discuss follow up procedures if a breach is not reported to the ICO. This should be documented alongside the record of the breach.

5. Reporting to the ICO

5.1 Where the ICO must be notified and this is agreed by the school, the DPO will do this within 72 hours. As required under Article 33 UK GDPR, the DPO will set out:

- A description of the nature of the personal data breach including, where possible;

- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the DPO;
- A description of the likely consequences of the personal data breach;
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

5.2 If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

5.3 The DPO will also assess the risk to individuals, based on the severity and likelihood of potential or actual impact. If the risk is high, and this is agreed by the school, the DPO will, without undue delay, inform all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the nature and likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- Where possible, advice to individuals to prevent adverse consequences from the breach

5.4 There is no legal requirement to notify the data subject if any of the following conditions are met:

- appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);
- measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

5.5 The DPO, if agreed by the school, will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

5.5 The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

5.6 Records of all breaches will be stored within the Trust's computer system on the Trust's breach spreadsheet and within the DPO's computer system. The DPO will not hold personal details contained in the breach where this is not necessary for the performance of their duties.

5.7 The DPO and Data Protection Lead will review the breach where necessary and how it can be prevented in future, as well as taking into account suggestions from the Trust Board.

6. Actions to minimise the impact of data breaches

6.1 We will ensure that staff have sufficient data protection training and ensure that the data protection policy is adhered to. We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. This may include amendments being made to the use of data processors and re-assessment as part of an ongoing Data Protection Impact Assessment.

7. Examples of actions to be taken in specific cases:

These are example scenarios. Trusts should be aware that breaches will be judged on a case-by-case basis in order for a fully informed decision and action to be implemented by the Truatl and the DPO.

7.1 Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask their point of contact to instruct the ICT department to recall it.
- In any cases where the recall is unsuccessful, the Data Protection Lead, with advice from the DPO, will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The Data Protection Lead, with advice from the DPO, will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- Further investigatory measures may need to be taken. A decision whether to inform the ICO and individuals effected will be carried out and documented.

7.2 Details of pupil premium interventions for named children being published on the Trust/School website.

- If the information is accidentally made available on a public domain, contact your website provider to ensure the data is removed. Seek advice from your IT services in order to recall the information and ensure its deletion.
- Contact your DPO and inform them of a breach on a website fixture. The DPO will carry out website checks to see if the information has been made public.
- In cases where the information has been posted for a period of time, the individuals who are affected will be contacted by the DPO and the ICO may be informed.

7.3 Non-anonymised pupil exam results or staff pay information being shared with governor and trustees.

- Contact the DPO who will ensure the governors/trustees are contacted and request a written response from governors/trustees ensuring the data's deletion.

- The DPO will ensure that this information has not been shared further.
- The DPO will conduct a review of the likely effect on individuals' rights and freedoms as to whether the breach will be furthered to the ICO and whether the individuals effected shall be informed.

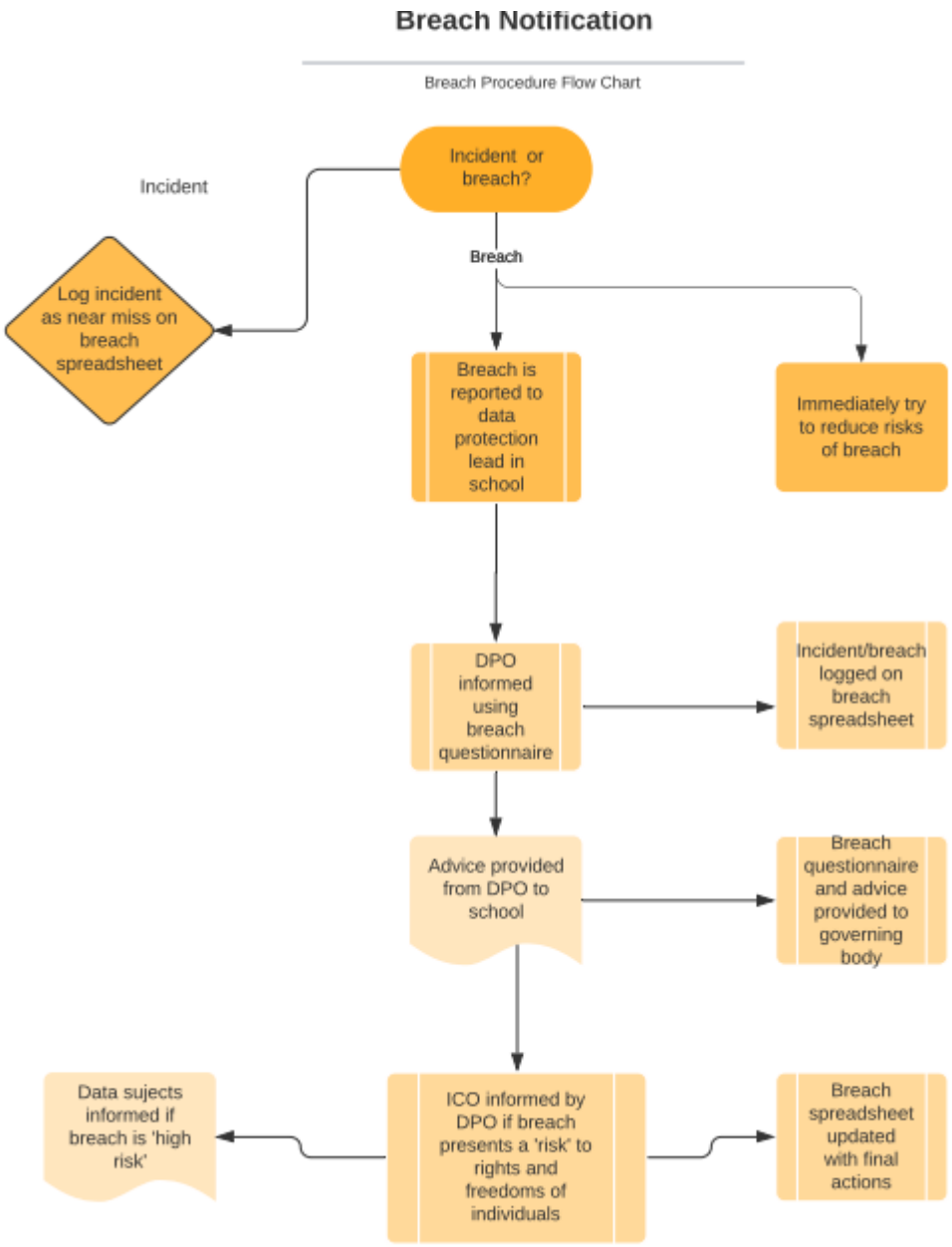
7.5 A School device containing non-encrypted sensitive personal data being stolen or hacked.

- The DPO should be informed in order to discuss the likely effect to the rights and freedoms of individuals whose personal data is stored on the device.
- Where an unencrypted device has been stolen or hacked, the protective measures within the device will be considered (i.e. password protections/storage of documents).
- The DPO will discuss with the IT team regarding the removal of personal data from the device, such as wiping the device.
- The DPO will discuss the likelihood of the return of the data and the device and the length of time the breach occurred in order to weight up the effect on individuals.

Preventative measures in all circumstances mentioned above will be reviewed and staff training will be enforced where necessary. Procedures and policies will be reviewed by the DPO in order to implement preventative measures.

Annex 1

Breach reporting flow diagram



Annex 2

Data Breach Reporting Form

Name:……

Role:……

Date and Time:……

Question	Answer
Date of the breach:	
When was the breach discovered:	
How was it discovered?	
Date and time reported to the DPO:	
Nature of the breach, including: Categories and approximate number of people whose data has been breached? Categories and approximate number of data records concerned?	
What has happened?	
How did it happen?	
Was this a human error or cyber error?	
If this was a cyber error please provide detail of the event including time limits, recovery information and which system was compromised.	
Did the person who committed the breach have GDPR training?	
What was the type of data included in the breach? (i.e. name, address, number)	
Was there any special category information within the breach? (such as medical information, ethnicity, TU membership, political opinion, race, sexual orientation, biometric/genetic information)	

What are the likely or actual consequences of the personal data breach to the individual? Are these judged to be significant consequences?	
Type of data subjects affected (employees/pupils/parents etc.)	
Measures you have taken or propose to take to address the breach, including measures to mitigate its effects?	
What measures were in place to prevent a breach occurring?	
What measures can be put in place to prevent this from occurring again?	
What has happened to the data now?	

Date:

DPO Advice: