Greater Nottingham Education Trust

Data Breach Policy

This policy will be reviewed by the Trust Board three yearly or amended if there are any changes in legislation before that time.

Date of last review: Summer 2021
Date of next review: Summer 2024

Policy Statement

The Greater Nottingham Education Trust holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

This procedure applies to all personal and sensitive data held by the Trust, all its academies and all employees, trustees, governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff within the Trust if a data protection breach takes place.

The Data Protection Officer is Mr Rod Bond-Taylor (mailto:DPO@gnetacademies.co.uk)

Legal Context

Article 33 of the UK General Data Protection Regulations (UK GDPR)
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe 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;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

A number of factors could cause data protection breaches. Examples could include:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access or security controls allowing unauthorised use;
- Equipment failure;
- Poor data destruction procedures;
- Human error such as accidental disclosure or release
- Cyber-attack;
- Hacking or phishing.

Managing a Data Breach

If an Academy of the Trust identifies or is notified of a personal data breach, the following initial steps will be taken:

1. The person who discovers the breach or receives a report of a breach must inform the Head Teacher (or, in their absence, the Deputy Head Teacher) and the Trust's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as IT Services.

3. The Head Teacher/DPO must inform the Chair of Governors as soon as possible. The Headteacher/DPO must also inform the nominated GNET trustee as soon as it appears that there is any likelihood of notification to ICO or to any individuals. As a registered Data Controller, it is an Academy's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the Trust's legal support should be obtained.

5. The Head Teacher/DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

   a) Attempting to recover lost equipment.

   b) A global email to all school staff members alerting them to the potential of receiving bogus enquiries (such as a phone call, email or other direct contact) resulting from the data breach . If such an enquiry is received, staff should attempt to obtain the bogus caller's name and contact details if possible and confirm that they will ring them back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO

   c) The use of back-ups to restore lost/damaged/stolen data.

   d) If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

   e) If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher/DPO to fully investigate the breach. The Head Teacher/DPO should ascertain whose data was involved in the breach; assess the extent of the damage, which may result, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The factors which will be considered in an investigation include:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO should, where appropriate, decide whether anyone needs to be notified of the breach. Unless the breach is unlikely to result in a risk to a person's rights and freedoms, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

Where the breach results in a high risk to a person's rights and freedoms, they must be notified that the breach has taken place. In addition, the Head Teacher/DPO must give specific and clear advice on what the individual can do to protect themselves and what the Academy/Trust is able to do to help them. The Head Teacher/DPO should also give the individual the opportunity to make a formal complaint if they wish (see the Academy's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved, as well as details of what has already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leaders Team, GNET and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to correct the identified problem. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or Head Teacher.

The Data protection Office is Mr Graham Johnson (mailto:DPO@gnetacademies.co.uk)

Section 1: Notification of Data Security Breach	To be completed by Head of Dept/School of person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known (or best estimate):	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery including any steps taken to address or mitigate impact of breach:	

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach.**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
What is the legal basis on which the information is held?	
What is the purpose for which the information is processed?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
What damage could arise in consequence of the breach and to whom?	
What is the likelihood of that damage arising?	
What is the likely severity of that damage?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Trust or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
Is the information sensitive? If so, what is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	

HIGH RISK personal data □ **Special category data** (as defined in GDPR) relating to a living, identifiable individual's a) racial or ethnic origin b) biometric data c) genetic data d) political opinions or religious or philosophical beliefs; e) membership of a trade union; f) physical or mental health or condition or sexual life or sexual orientation g) commission or alleged commission of any offence, or h) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
□ Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
□ Personal information relating to vulnerable adults and children;	
□ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
□ Spreadsheets of marks or grades obtained by students, information about individual cases of	
□ Student discipline or sensitive negotiations, which could adversely affect individuals.	
□ Security information that would compromise the safety of individuals if disclosed.	
Which Article 9 (2) exemption applies allowing use of this special category of data?	
Is notification to ICO required? Answer YES unless the breach is unlikely to result in a risk to a person's rights and freedoms"	
Is notification to any person(s) required? Answer YES if the breach results in a high risk to their rights and freedoms"	

Section 3: Action taken	To be completed by Data Protection Officer and/or Lead Investigation Officer
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	

For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**