

# David Nieper Education Trust



## Data Breach Procedure

---

This policy was originated by Joy Williams, Business Manager

### Version Control

Version 1	Approved by Governing Body Autumn 2018
Version 2	Reviewed & Approved Autumn 2019
Version 3	Reviewed and updated Spring 2021

Signed:	Date:

**Due for review Spring 2023**

# **David Nieper Academy Data Breach Procedure**

## **Purpose**

David Nieper Academy 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 David Nieper Academy and all academy staff, Governors, Trustees, volunteers, and contractors, referred to herein after as 'staff'.

This breach procedure sets out the course of action to be followed by all staff at **David Nieper Academy** if a data protection breach takes place.

## **Legal Context**

### **Article 33 of the General Data Protection Regulations 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**

Data protection breaches could be caused by several factors. A few examples are shown below:

- Loss or theft of student, staff, or governing body data and/ or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment Failure preventing access to information or causing a loss of personal data required for the operations of the academy.
- Poor data destruction procedures.
- Human Error.
- Cyber-attack.
- Hacking.

## **Managing a Data Breach**

In the event that the Academy identifies or is notified of a personal data breach, the following steps should follow:

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

Contact the Headteacher at [info@davidnieper.academy](mailto:info@davidnieper.academy)  
Contact the DPO at [dp@agilecls.co.uk](mailto:dp@agilecls.co.uk)

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 the IT technician.
2. Where the Head Teacher or their nominated representative is notified of a breach, and as soon as minimisation actions are underway, they should inform the Data Protection Officer. The Data Protection Officer will review the facts as known and undertake an initial assessment of risk and impact to inform subsequent actions and advise on the need to notify the Information Commissioners Office (ICO).

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Trustees as soon as possible. As a registered Data Controller, it is the academy's responsibility to take the appropriate action and conduct any investigation.
4. The Head Teacher/DPO (or nominated representative) 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 Academy's legal support should be obtained.
5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
  - a. Attempting to recover lost equipment.
  - b. Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all academy staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).
  - c. Contact the Academy PR support so they can assist with any press enquiries.
  - d. The use of back-ups to restore lost/damaged/stolen data.
  - e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
  - f. 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 (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- 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 (students, 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. Initial investigations, to allow a decision to be made regarding notifications (see below) should therefore be completed within the first 48 hours after a breach is discovered. 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 (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, 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.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the Academy is able to do to help them. You should also give them 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. Include details of what you have already done to mitigate the risks posed by the breach.

### **Review and Evaluation**

Once the initial risks associated with the breach have been contained, the Head Teacher/DPO (or nominated representative) 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 Management Team and Finance, Audit and Risk Committee meetings for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with the Head Teacher, who will work with the Academy HR advisor if required 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 Academy's 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 Academy's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.