NORTHAMPTON
PRIMARY ACADEMY TRUST

NPAT Data Breach Policy
AND PROCEDURE

Associated Policies:	Complaints policy GDPR policy Online safety policy Records management and retention policy Subject access request policy
Author:	Executive Office Manager
Date Approved:	16th Dec 2024
Approved by:	Board of Trustees
Date issued:	14th January 2025
Date of Next Review:	Nov 2027
Website Inclusion	N
Version:	1.1 25

CONTENTS

Northamptonshire Primary Academy Trust is proud to produce written materials that consider the British Dyslexia Association style guide principles.

1. POLICY STATEMENT

1.1 Northampton Primary Academy Trust (NPAT) is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.2 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

1.3 All members of our **workforce**, governors, contractors, consultants and suppliers must understand and comply with this policy when **processing** personal data on our behalf and are responsible for ensuring the safety and security of systems and information. Any breach of this policy may result in disciplinary or other action.

1.4 This policy and procedure is based on guidance on personal data breaches produced by the Information Commissioners Office (ICO)

1.5 The purpose of this policy and procedure is to ensure that our Trust and schools react appropriately to mitigate the risks associated with security incidents relating to data.

2. WHO DOES THIS POLICY APPLY TO

2.1 This policy applies to all NPAT Staff, Volunteers, Governors, contractors, consultants and suppliers.

3. POLICY REVIEW ARRANGEMENTS

This policy will be reviewed and updated as necessary if/when any changes are made to legislation that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed every 3 years.

4. ABOUT THIS POLICY

4.1 In the event of a suspected or identified breach, NPAT must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

4.2 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

4.3 The Trust must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose personal data has been adversely affected and are at high risk by the breach. This includes any communications with the press.

4.4 Failing to appropriately deal with and report data breaches can have serious consequences for the Trust and for data subjects including:

4.4.1 identity fraud, financial loss, distress or physical harm;

4.4.2 reputational damage to the Trust; and

4.4.3 fines imposed by the ICO.

5. RESPONSIBILITIES

The Trust has overall responsibility to put in place clear policies and procedures.

5.1 **Trust Board**

The Trust Board has overall responsibility for ensuring that schools with the Trust comply with all relevant data protection obligations.

5.2 **Data Protection Officer**

The Data Protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, maintaining breach and incident logs and supporting and advising the Trust Executive Office and schools.

5.3 **Trust Executive Office**

The Trust Executive Office will retain central records of breach and incident logs and meet regularly with the Trust DPO to review breach records.

5.4 **Headteacher**

The Headteacher has overall responsibility for GDPR and data protection within their school.

5.5 **All staff, volunteers and Governors**

Are responsible for complying with the policy and procedure and notifying the DPO of any suspected data breaches as quickly as possible.

6. DEFINITION OF DATA PROTECTION TERMS

6.1 All defined terms in this policy are indicated in bold text, and a list of definitions is included in Appendix 2.

7. IDENTIFYING A DATA BREACH

7.1 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.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

So, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

7.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data.

Some examples of potential data breaches are listed below: (This list is not exhaustive)

- Leaving a mobile device on a train;
- Theft or loss of a bag containing paper documents;
- Destruction of the only copy of a document;
- Using an unauthorised email address to access personal data;
- Leaving paper documents containing personal data in a place accessible to other people;

- Emailing documents containing personal data to incorrect or unauthorised recipients;
- Sharing template documents pre-populated with personal data;
- Disclosing personal data by displaying it in inappropriate locations such as walls or notice boards;
- Providing hard copy reports to wrong pupils / families;
- Publishing details of pupil premium interventions for named children on school websites;
- The school's cashless payment provider being hacked and parents' financial details stolen;
- Writing down passwords and leaving them accessible to others;
- Accessing a computer database using someone else's authorisation / password.
- Sharing pupil images on social media where a parent has not provided explicit consent

8. INTERNAL COMMUNICATION

8.1 Reporting a data breach upon discovery

If any member of NPAT suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our workforce, a data processor, or any other individual) then they must contact the Trust Data Protection Officer ("the DPO") immediately by email at: dpo@npatschools.org

The data breach may need to be reported to the ICO and notified to data subjects. This will depend on the risk to the data subjects.

The DPO is responsible for making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

If it is considered to be necessary to report a data breach to the ICO then the Trust must do so within 72 hours of discovery of the breach. The DPO holds responsibility for submitting the report to ICO.

The Trust may also be contractually required to notify other organisations of the breach within a period following discovery.

It is therefore critically important that whenever a member of our workforce suspects that a data breach has occurred, this is reported to the DPO immediately. Please ensure the personal data breach form is completed providing as much information as possible to support with the investigation and containment of the breach.

Members of NPAT who fail to report a suspected data breach could face disciplinary or other action.

8.2 Investigating a suspected data breach

The Trust DPO will investigate 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 visible where it should not have been
- Made available to unauthorised people
- Made unavailable, with a significant negative effect on individuals

In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Staff, volunteers and governors are expected to cooperate with the breach investigation as directed by the Trust DPO.

The Trust DPO is responsible for maintaining and updating the Trust Data Breach and incident Log(s) and for notifying the Trust Executive Office of any Data Breach investigations.

8.3 Breach minimisation

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:

- Where special category data (sensitive information) is accidentally made available by 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 report to the DPO as soon as they become aware of the error;

- Remote deactivation of mobile devices where possible;

- Shutting down IT systems;

- Contacting individuals to whom the information has been disclosed and asking them to delete the information; and endeavour to obtain a written response to confirm they have complied with this request;

- Carrying out an internet search to check that the information has not been made public where appropriate to do so and contacting the publisher/website owner to request removal and deletion.

- Where safeguarding information is compromised, the DPO will inform the designated safeguarding lead and consider if the school should inform any or all of its local safeguarding partners.

- Recovering lost data.

The Trust DPO will provide guidance on all reasonable efforts to contain and minimise the impact of the breach.

8.4 Breach investigation:

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 re-occurring.

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

8.5 Breach analysis

In order to determine the seriousness of a data breach and its potential impact on data subjects, and so as to inform the Trust as to whether the data breach should be reported to the ICO and notified to data subjects, to the Trust DPO will analyse the nature of the data breach using the ICO's self-assessment tool

Such an analysis must include:

- The type and volume of personal data which was involved in the data breach;
- Whether any special category personal data was involved;
- The likelihood of the personal data being accessed by unauthorised third parties;
- The security in place in relation to the personal data, including whether it was encrypted;
- The risks of damage or distress to the data subject.

The personal data breach form (**Appendix 1**) must be completed initially by the school for every case of a suspected breach. This will be added to form a report by the DPO, and retained securely, whether or not a decision is

ultimately made to report the data breach. This will act as evidence as to the considerations of the Trust in deciding whether or not to report the breach.

9. EXTERNAL COMMUNICATION

All external communication will be overseen by the DPO.

9.1 Law enforcement

The DPO will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

DPO shall coordinate communications with any law enforcement agency.

9.2 Other organisations

If the data breach involves personal data which we process on behalf of other organisations then we may be contractually required to notify them of the data breach.

The Trust will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

9.3 Information Commissioner's office

If the Trust is the data controller in relation to the personal data involved in the data breach, which will be the position in most cases, then the Trust has 72 hours to notify the ICO if the data breach is determined to be notifiable.

A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

- the type and volume of personal data which was involved in the data breach;
- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;

- the risks of damage or distress to the data subject.

If a notification to the ICO is required then see part 7 of this policy below.

9.4 Other supervisory authorities

If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

9.5 Data subjects

When the data breach is likely to result in a high risk to the rights and freedoms of the data subjects then the data subject/s must be notified without undue delay.

This will be informed by the investigation of the breach by the Trust.

The communication will be coordinated by the DPO and will include at least the following information;

- a description in clear and plain language of the nature of the data breach;
- the name and contact details of the DPO;
- the likely consequences of the data breach;
- the measures taken or proposed to be taken by the Trust to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

There is no legal requirement to notify any individual 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;

- it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

For any data breach, the ICO may mandate that communication is issued to data subjects, in which case such communication must be issued.

9.6 Press

Members shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

All press enquiries shall be directed to the Headteacher/Trust Executive Team.

10. PRODUCING AN ICO BREACH NO

The Trust DPO is responsible for notifying appropriate cases to the ICO.

The DPO will report the breach using the online data breach form at: ICO Online data breach form

11. EVALUATION AND RESPONSE

Reporting is not the final step in relation to a data breach. The Trust will seek to learn from any data breach.

Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of NPAT to reinforce good practice, or providing additional training, or may in more serious cases require disciplinary processes, new technical systems and processes and procedures to be put in place.

The Trust DPO and Executive Office Manager will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

12. TRAINING

All NPAT staff will be provided with data protection training as part of their induction to the Trust.

Data protection will also form part of continuing professional development, where changes in legislation, guidance or Trust processes make it necessary.

Appendix 1 **Personal Data Breach Processing Form.**

<table>
<tr><td>Academy/Trust name</td><td></td></tr>
<tr><td>Designated Academy/Trust contact reporting the breach</td><td>Name:

Email:

Contact No:</td></tr>
<tr><td>Description about Personal Data breach</td><td>Description of breach:

<table>
<tr><td>Date it happened</td><td></td></tr>
<tr><td>How did the breach get identified and date?</td><td></td></tr>
<tr><td>Pupil personal data shared including the number affected</td><td></td></tr>
<tr><td>Parent/carer personal data shared including the number affected</td><td></td></tr>
<tr><td>Staff personal data shared including the number affected</td><td></td></tr>
<tr><td>Others affected by the breach, governors, external people</td><td></td></tr>
<tr><td>Please detail any immediate action take</td><td></td></tr>
<tr><td>Date reported to DPO</td><td></td></tr>
<tr><td>Staff members involved in the breach, when did they last complete GDPR training</td><td></td></tr>
</table>
</td></tr>
</table>

To be completed by DPO:	
Personal data breach notified to DPO **(within 24 hours)**	**Date:**
DPO reports to Central team (if required)	**Date:** **Who:**
DPO to assess the extent of the breach **(within 48 hours)**	**The risks to the data subjects (individuals) as a consequence of the breach:** **Any security measures in place that will protect the information:** **Measures taken immediately to mitigate the risk to the individuals:**
If the breach identifies high risk to adversely affect individuals, they must be notified without undue delay	**If yes, please record the date and how notified (including number of individuals):**
DPO concludes whether to report to ICO	**If yes, please record the date:** **If no, reasons why:**
Record Data Breach on Trust log	**Date:**
DPO instigates investigation into the breach	**A report will be produced if a significant breach:** • How it happened? • Whether it could have been prevented? • Recommendations for further training and procedure changes if required
Actions	

Appendix 2 **Definitions**

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by NPAT such as staff and those who volunteer in any capacity including Governors [and/or Trustees / Members/ parent helpers]