Personal Data Breach Procedure

Applicable to:	✓	All individual academies within NEAT
	×	Specified academies only
	✓	NEAT Trust
Approval body:	NEAT Board of Directors	
Effective date:	24 May 2018	

Status:

Statutory policy or document	No
Review frequency	As determined by the Board
Approval by	As determined by the Board

Publication:

Statutory requirement to publish on website	No
If not, agreed to publish on website?	No

Version Control:

Revision Record of Issued Versions			
Author	**Creation Date**	**Version**	**Status**
Central Support Manager (SH)	24 May 2018	1.0	Agreed by Board of Directors for implementation across the Trust.
Changed by	**Revision Date**	**Version**	**Status**

Review Date	
Frequency	**Next Review Due**
Every three years	May 2021 (or earlier if new guidance or legislation issued and/or business need for earlier review identified)

1 Purpose

The purpose of this procedure is to set out how NEAT and its academies will detect, investigate and report personal data breaches.

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. It includes breaches that are the result of both accidental and deliberate causes.

2 Scope

The procedure applies to the trust and all of its academies. It covers the trust's employees, any authorised agents working on behalf of the trust, including temporary or agency staff, volunteers, directors/trustees, local governors and third party contractors.

This procedure applies to information in all forms including, but not limited to:

- hard copy or documents printed or written on paper;
- information or data stored electronically, including scanned images;
- communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- speech, voice recordings and verbal communications, including voicemail;
- published web content, for example intranet and internet; and
- photographs and other digital images.

Examples of personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

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.

4 Legal considerations

This policy is to ensure that the trust and its academies comply with the requirements of the Data Protection Act 2018, associated guidance and Codes of Practice issued under the legislation. Failure by the trust to notify a breach to the Information Commissioner's Office when required to do so can result in a significant fine.

5 Roles and responsibilities

- **Trust's Board of Directors:** The Trust Board will review this policy and evaluate its effectiveness. The Audit, Risk and Finance Committee has oversight of any risks arising from information governance.

- **Information asset owners (IAO):** An IAO is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it, as set out in the trust's Data Protection Policy.

- **Specific point of contact (SPOC):** The NEAT Governance Support Adviser acts as the specific point of contact on behalf of the trust and its academies. All data breaches or information security events must be notified to this person. They also ensure investigations into data breaches have identified all potential information risks and that remedial actions have been implemented.

- **Senior information risk owner (SIRO):** The NEAT Director of HR and Governance acts as the senior information risk owner on behalf of the trust and its academies. The SIRO, in conjunction with the Headteacher/CEO, SPOC, IAO and DPO will make a decision as to whether an incident needs to be reported to the Information Commissioner's Office, and also whether any data subjects need to be informed. They are also responsible for reviewing investigations into data breaches and ensuring recommendations are implemented across the trust and its academies.

- **Data Protection Officer (DPO):** The Data Protection Officer appointed by the trust is: Veritau Ltd, Information Governance Team, County Hall, Racecourse Lane, Northallerton DL7 8AL Tel: 01609 532526 E-mail: schoolsDPO@veritau.co.uk . The DPO is a statutory position and operates in an advisory capacity. Their duties include assisting with the reporting and investigation of information security breaches.

- **All employees and authorised agents acting on behalf of the trust:** Failure to deal with personal data breaches as set out in this procedure may result in actin under the trust's Disciplinary Procedure for employees, or the trust reviewing its ongoing relationship with agency staff, third party contractors, local governors and directors/trustees.

6 Notification and containment

Data controllers must report breaches of personal data to the Information Commissioner's Office within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of data subjects.

6.1 Immediate actions (within 24 hours)

If any individual within scope of this procedure is made aware of an actual data breach, or an information security event (or "near-miss"), they must report it to their line manager (or Chair of the Trust Board in the case of directors/trustees and local governors) and the trust's specific point of contact (SPOC) within 24 hours. If the SPOC is not at work at the time of the notification then their out-of-office email will nominate another individual to start the investigation process.

If appropriate, the person who located the breach, or their line manager, will

make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

The SPOC will record all data breaches and information security events on behalf of the trust, regardless of whether they need to be notified to the Information Commissioner's Office, and document the effects and remedial action taken.

6.2 Assigning investigation (within 48 hours)

Once received, the SPOC will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

WHITE	**Information security event** No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future i.e. a "near miss. For example, a letter containing personal information being sent to the incorrect address that was either returned unopened or retrieved prior to being opened.
GREEN	**Minimal impact** A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary. For example, a letter or email containing the personal details of a pupil being sent to the incorrect social worker or health professional; an e-mail sent to parents cancelling an after school club when the "blind copy" or "bcc" function has not been used.
AMBER	**Security impact** Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the Information Commissioner's Office. For example, information posted or emailed to the incorrect parent/member of the public that reveals personal or potentially sensitive data about a pupil and remedial action is necessary to mitigate any potential risk e.g. taking swift action to retrieve any erroneous documentation and informing the individuals concerned.
RED	**Serious impact** A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the Information Commissioner's Office and urgent remedial action. For example, extremely sensitive information regarding a pupil/their family (such as adoption status of the child or conviction history of a parent) has been sent to the incorrect parent/member of the public, or the loss or theft of an unecrypted device which holds a database detailing all the children in the school who are "looked after" or details SEN provision.

The SPOC will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The SPOC will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit as necessary.

6.3 Reporting to the ICO/informing data subjects (within 72 hours)

The SIRO, in conjunction with the Headteacher/CEO, SPOC, IAO and DPO will decide whether the breach needs to be reported to the ICO. They will also decide whether any data subjects need to be informed without undue delay.

The Headteacher/CEO and the IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

7 Investigating and concluding incidents

The SPOC will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the SIRO must sign off the investigation report and ensure recommendations are implemented across the trust and its academies.

The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

General
In the event of any conflict with primary legislation or statutory regulations, the legal provisions will have precedence over this policy in all cases.