Data Security Breach Policy

Policy Document Control Sheet:

Trust lead: Ian Hickman

Key Staff lead for The Blyth Academy: Andrew Buxton – ICT & Network Manager & Caroline Turner – Operations Manager

Portfolio Governor lead: David Hall

Status: Agreed and adopted

Date	Process	Category
Jan to Feb 2017	**Consultation period**	
17th February 2017	**Approved by Stakeholders**	
24th March 2017	**Approved by NET Trust Board**	
5th December 2017	**Adopted by LGB**	
March 2019	**Next review date**	Discretionary: NET/Local

1. Introduction

1.1 The Trust holds a large amount of data / information, both in hard and soft copy. This includes personal or confidential information (about people), and also non-personal information which could be sensitive or commercial, for instance financial data, performance reviews and similar information.

1.2 Care should be taken to protect this type of data / information, to ensure that it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands, that its authenticity and integrity is maintained.

1.3 In the event of a breach, it is vital that appropriate action is taken to minimise associated risks.

2. What is a breach?

A data breach is an incident in which any of these types of data specified in 1.1 above is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples include:

- Accidental loss, or theft of equipment on which data is stored or of the paper copies
- Unauthorised access to data
- Human error such as emailing data by mistake
- Failure of equipment and hence data held on it
- Loss of data or equipment through fire or flood, for instance
- Hacking attack
- Where information is obtained by deceiving a member of staff

3. Reporting of the breach

3.1 Data security breaches should be reported immediately to the Chief Operating Officer, or his nominated Officer, as the primary point of contact. The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved.

Contact details: **Andy Thom**, **Trust Secretary**, tel. **0191 594 5149**

Email: andy.thom@northerneducationtrust.org

4. Investigation and Risk Assessment

4.1 The Chief Operating Officer, or his/her nominated Officer, will instigate a response in accordance with the Trusts ICM Plan, this will include a named officer, who will be responsible for investigating data breaches. An investigation will be started within 24 hours of the breach being discovered, where possible.

4.2 The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals, and if so who are the subjects and how many are involved.

4.3 The investigation will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to the institution.

5. Containment and Recovery

5.1 The Team will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.

5.2 Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

5.3 Advice from experts across the Trust or from external organisation with relevant expertise may be sought.

6. Notification

6.1 The Chief Operating Officer will be notified by the Team following a critical data breach involving large amounts of data, or a significant number of people whose personal data has been breached. S/he will make a decision based on the seriousness of the breach to notify the Chief Executive and/or Chair of the Trust Board.

6.2 The Chief Operating Officer will make a decision to inform any external organisation, such as the police or other appropriate regulatory body, currently this is the ICO.

6.3 If a personal data breach has occurred, the Information Governance Officer will be informed. S/he will inform the Information Commissioner's Office if necessary, based on the extent of the breach.

6.4 Notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks, and will be undertaken by the Team.

7. Review

7.1 Once the breach is contained a thorough review of the event will be undertaken by the Team, to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement.

7.2 Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible after consultation with Trustees.

8. Reporting

8.1 The GDPR will introduce a duty on all organisations to report certain types of data breach to the ICO, and in some cases to the individuals affected.

8.2 Notifiable breaches must be reported to the ICO within 72 hours of the Trust become aware of the breach. Failure to do so can result in a significant fine.

8.3 Each case will need to be assessed on a case by case basis and advise sought from the Trust Data Protection Officer and/or the ICO.

8.4 It is anticipated the ICO will issue further guidance in this area as we approach May 2018.

9. Relevant links

Information Commissioner – www.ico.org.uk

10. Relevant legislation

Data Protection Act 1998

General Data Protection Regulations 2018 (effective from 25th May 2018)