John Spence
COMMUNITY HIGH SCHOOL

Data Breach Reporting Policy 2023

Information Governance Team
Version 1.0

1.0 Introduction

John Spence Community High School holds, processes and shares a large amount of personal data, a valuable asset that needs to be protected.

Every care is taken to protect personal data and avoid a data protection breach (either accidental or deliberate).

Compromise of confidentiality, integrity, or availability of information may result in harm to individuals, reputational damage, a detrimental effect on service provisions, legislative non-compliance and financial costs.

2.0 Purpose

JSCHS is obliged, under the Data Protection Legislation, to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breaches and information security incidents across the school.

3.0 Scope

This policy relates to all personal data held by the JSCHS regardless of format.

This policy applies to all staff and contractors at the school. This includes teaching staff, temporary, casual and agency staff, suppliers and data processors working for or on behalf of the school.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what remedial action is necessary to secure personal data and prevent further breaches.

4.0 Definition/types of breach

An incident, in the context of this policy, is an event which may compromise the confidentiality, integrity or availability of systems or data, either

accidentally or deliberate and has caused or has the potential to cause damage to the school's information assets and/or reputation.

An incident includes but is not restricted to, the following:-

- Loss or theft of personal data or equipment on which such data is stored (e.g loss of a laptop, iPad/Tablet, mobile device or paper record).
- Unauthorised use, access to (either successful or failed) or modification of data or information systems
- Unauthorised disclosure of personal data (either deliberate or accidental)
- Offences where information is obtained by deceiving the organisation who holds it.

5.0 Reporting an incident

Any individual who accesses, uses or manages the school's data is responsible for reporting any data breach and information security incidents immediately to Melissa.Tunney@Johnspence.org.uk (designated senior management position within the school). If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable.

The incident should be recorded on a data breach log, which should include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, how many people are involved, and, following the investigation, information on how similar incidents will be avoided in the future.

The school's Data Protection Officer (DPO) can be contacted at dpo.schools@northtyneside.gov.uk or 0191 643 2333 for advice and guidance.

6.0 Containment and recovery

The designated person will firstly determine if the breach is still occurring and if so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made with relevant officers to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach; in some cases it could be the DPO).

Containment of the breach may involve requesting that the recipient of information that has been mistakenly disclosed, returns or deletes this document.

7.0 Investigation, Risk Assessment and Notification

An investigation will be undertaken by the designated person immediately and where possible within 24 hours of the breach being discovered/reported.

This person will investigate the breach and assess the risks associated with it, for example, the potential adverse effects for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:-

- The type of data involved
- It's sensitivity
- The protection in place (e.g. encryption)
- What's happened to the data, has it been lost or stolen
- Whether the data could be put to illegal or inappropriate use
- Who are the affected individuals, the total number affected and the potential effects on those data subjects
- Whether there are wider consequences to the breach

The above investigation points will help determine whether the data subject/s need to be made aware of the breach, and if it needs to be reported to the Information Commissioner.

If the breach is likely to adversely affect individuals, then we will notify the data subjects without undue delay. This notification will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the school for further information.

If it is felt that the risks to individuals are high, the ICO will be contacted, with all of the above information, within 72 hours of discovering the breach.

Consideration will be given as to the necessity to notify third parties such as the Police, insurers and banks. 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.

Consideration will also be given as to whether any press release may be required.

All actions will be recorded on the data breach log

9.0 **Evaluation and response**

Once the initial incident is contained, a full review will be carried out examining the causes of the breach, the effectiveness of the response and whether any changes to systems, policies or procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:-

- Where and how the personal data is held and where it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure, sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.