Data Breach Policy and Procedure

1. Introduction

1.1 The Gosforth Federated Academies Limited holds, processes and shares a large amount of personal data, a valuable asset that needs to be protected.

1.2 Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

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

2. Purpose and scope

2.1 The Trust is obliged under the Data Protection Act 2018 and the UK General Data Protection Regulation to have in place a framework designed to ensure security of all personal data during its lifecycle, including clear lines of responsibility.

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

2.3 This policy relates to all personal and special category data held by the Trust regardless of format

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

2.5 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.

3. Definition / types of breach

3.1 For the purposes of this policy, data security breaches include both confirmed and suspected incidents.

3.2 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 deliberately and has caused or has the potential to cause damage to the Trust's information assets and/or reputation.

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

- Loss or theft of confidential or special category data, or equipment on which such data is stored (e.g. loss of a laptop, memory stick, iPad/Tablet, or paper record;
- Equipment theft or failure;
- Unauthorised use, access, or modification of data or information systems;
- Attempts (failed or successful) to gain unauthorised access to information or IT systems;
- Unauthorised disclosure of special category and confidential data;
- Website defacement;
- Hacking attack;
- Unforeseen circumstances such as a fire or flood;
- Human error;
- Blagging offences where information is obtained by deceiving the organisation who holds it.

4. Reporting an incident

4.1 Any individual who accesses, uses or manages the Trust's data is responsible for reporting the data breach and information security incidents immediately to the school designated contact.

4.2 This will trigger a report to the Trust's appointed Data Protection Officer at dataservices@judicium.com.

4.3 If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. The Trust has only 72 hours to report a breach to the Information Commissioner's Office.

4.4 The report will include full and accurate details of the incident, when the breach occurred details of the person reporting the breach, whether the breach relates to people, the nature of the information, and how many people are involved. A Data Breach Report Form should be completed as part of the reporting process. A template report should be obtained from the DPO.

5. Containment and recovery

5.1 The Data Protection Officer will firstly determine if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach.

5.3 The Lead Investigation Officer (LIO) will establish who may need to be notified as part of the initial containment and will inform the police, if appropriate.

5.4 The LIO, in liaison with the relevant officers will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1 An investigation will be undertaken by the LIO immediately and where possible within 24 hours of the breach being discovered or reported.

6.2 The LIO 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.

6.3 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 the individuals are, the number affected and the potential effects on those data subjects;
- Whether there are wider consequences to the breach.

7. Notification

7.1 The LIO and/ or the DPO, in consultation with the Principal will determine whether the breach needs to be reported to the Information Commissioner's Office.

7.2 Every incident will be assessed on a case by case basis against the following considerations:

- Whether there are any legal or contractual notification requirements;
- Whether notification would assist the individual affected – could they act on information to mitigate the risks;
- Whether notification would help prevent the unauthorised or unlawful use of personal data;
- Would notification help the Trust meet its obligations under the principle;
- Whether this breach constitutes a high risk to individuals and therefore needs to be reported to the ICO.

7.3 Notification to the individuals whose personal data has been affected by the incident 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 Trust for further information or to ask questions about what has occurred.

7.4 The LIO and/ or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. 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.

7.5 The LIO and/ or DPO will consider whether any press release may be required.

7.6 All actions will be recorded by the LIO and DPO.

8. Evaluation and response

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

8.2 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.

8.3 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 the 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