George Stephenson High School

DATA BREACH POLICY

Governance	Curriculum Committee Governing Body
Policy Officer	Assistant Headteacher (Data)
Adopted Date	November 2018
Review Date	3 February 2021
Next Review Date	February 2024

CONTENTS PAGE

1. Introduction 3
2. Purpose 3
3. Scope 3
4. Definition/types of breach 3
5. Reporting an incident 4
6. Containment and recovery 4
7. Investigation and Risk Assessment 4
8. Notification 4
9. Evaluation and response 5
APPENDIX 1 6
DATA BREACH REPORT FORM 6

1. Introduction

As a Data Controller, we hold, process and share a large amount of personal data which is a valuable asset that needs protected. We take every care to protect personal data from incidents (either accidental or deliberate) and to avoid a data protection breach that could compromise the security or integrity of the information we hold.

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 that has caused or has the potential to cause damage to our information assets. 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

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

This policy sets out the procedure to be followed in the event of an incident to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

3. Scope

This policy relates to all personal and special category data held by us, regardless of format This policy applies to all staff, including temporary workers or volunteers, and contractors. This includes teaching students, casual, agency staff, suppliers and data processors working for or on our behalf.

The objectives of this policy are to;

- contain any breaches
- minimise the risk associated with the breach
- implement remedial action if necessary to secure personal data
- prevent further breaches.

4. Definition/types of breach

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

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 of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or I.T systems
- Unauthorised disclosure of special category/ confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire of flood
- Human Error
- Blagging offences where information is obtained by deceiving the organisation who holds it.

5. Reporting an incident

Any individual who accesses, uses or manages personal data on our behalf is responsible for reporting any data breach and information security incidents immediately to us via styson@gshs.org.uk We will inform our Data Protection Officer, Judicium Consulting Limited, dataservices@judicium.com of all breaches reported to us.

If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. We must report data breaches that result, or are likely to result, in high risk to the rights and freedoms of individuals to the Information Commissioner with undue delay and in any event within 72 hours from the time we become aware of the beach. All Staff must therefore ensure any actual or suspected breaches are reported as soon as possible.

Any reports must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information and how many people are involved are affected.

An incident reporting form (Appendix 1) should be completed as part of the reporting process.

6. Containment and recovery

The Data Protection Officer will advise whether, in their opinion, the breach is still occurring. If so, appropriate steps agreed with the DPO must be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach. A Lead Investigation Officer (LIO) will be nominated who will take the lead investigating the breach and liaising with the DPO.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police if required and where appropriate.

The DPO and LIO will in liaison determine the suitable course of action to be taken to ensure a resolution to the incident.

7. Investigation and Risk Assessment

An investigation will be undertaken by the LIO immediately and where possible within 24 hours of the breach being reported. The DPO will assist where required.

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.

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

8. Notification

The LIO and the DPO will determine whether the breach needs to be reported to the Information Commissioner or the data subjects affected.

Every incident will be assessed on a case by case basis; however, the following will need to be considered: -

- Whether there are any legal/contractual notification requirements
- Whether notification would assist the individual affected
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Whether this breach constitutes a high risk to individuals

Notification to the individuals whose personal data has been affected by the incident will only be necessary in circumstances where there is a high risk to that person as a result of the breach. Any such notifications must include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on potential steps they can take to protect themselves, and the notification will include details of what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the DPO for further information or to ask questions about what has occurred.

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

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

All actions taken or required to be taken will be recorded by the LIO and DPO.

9. Evaluation and response

Once the initial incident is contained, the DPO will, upon request, 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.

As soon as possible after a breach, the LIO should liaise with the DPO to review existing controls 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 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

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches.

If you discover a data breach, please notify the leadership team immediately and report it via styson@gshs.org.uk who will then inform dataservices@judicium.com

Report details:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Date of report:	
If there has been a delay in reporting this breach to the DPO, please explain why:	

Details of the Breach:	
What has happened? Tell us as much as you can about what happened, what went wrong and how it happened.	
How did you find out about the breach?	
When was the breach discovered? Please include date and time	
When did the breach happen? Please include date and time where possible	
Categories of personal data involved in the breach: Please list all categories of data that have been affected	*E.g.: name, address, bank details, UPN, SEN Information, Assessments etc*
Number of personal data records concerned?	
How many data subjects could be affected?	
Categories of data subject affected?	*E.g.: students (current and past), staff, volunteers*

Potential consequences of the breach: Please describe the possible impact on data subjects because of the breach. Please state if there has been any actual harm to the data subjects	
What is the likelihood that the data subjects will experience consequences because of the breach?	□ Very Likely □ Likely □ Neutral □ Unlikely □ Very Unlikely □ Not yet known
Has the staff member involved in this breach received data protection training in the last two years? Include date if yes	

Action Taken:	
Describe the actions you have taken or proposed to take as a result of the breach: Include actions you have taken to fix the problem and to mitigate any adverse effects	
Date action taken or proposed to be taken:	

Cyber Incidents only:	
Has the confidentiality, integrity or availability of information systems been affected? Identify which if applicable	
What is the impact of this?	□ **High** – have lost ability to provide critical services □ **Medium** – have lost ability to provide some critical □ **Low** – no loss of efficiency and can still provide all critical services □ **Not yet known**
Likely recovery time:	□ **Complete** – recovery is fully complete □ **Regular** – you can predict recovery time with existing resources □ **Supplemented** – you can predict recovery time with additional resources □ **Extended** – you cannot predict recovery time and need extra resources □ **Not Recoverable** – recovery is not possible, e.g. backups can't be restored □ **Not yet known**

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	
Incident number	**e.g. year/001** *Use Iken Ref when available*
Follow up action required/recommended:	
Notification to ICO advised?	**YES/NO** **If YES, notified on:** **Details:**
Notification to data subjects advised?	**YES/NO** **If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder advised?	**YES/NO** **If YES, notified on:** **Details:**
Notification to police advised?	**YES/NO** **If YES, notified on:** **Details:**