Data Breach Reporting

Policy Statement 2022-2024

The best interests of the child must be a top priority in all decisions and actions that affect children (Article 3).

We must respect the rights and responsibilities of parents and carers to provide guidance and direction to their child as they grown up, so that they fully enjoy their rights (Article 5)

Every child has the right to privacy (Article 16)

UN Convention on the Rights of the Child

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 harlowgreenprimaryschool@gateshead.gov.uk We will inform our Data Protection Officer, Veritau Ltd, 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

Information Security Incident Reporting and Investigation Form

Do not provide personal details of those involved or affected by a data breach. E.g. refer to them as pupils, service users, parents etc.

Stage 1: Initial recording and reporting of the incident

If you discover a data breach, please notify the Head Teacher or Business Manager immediately and report it via harlowgreenprimaryschool@gateshead.gov.uk

You should use this report to record your breach in full.

You will need to complete all the boxes in this report to ensure the school has a full record of the breach and all actions taken.

Part 1 - About the incident	
Date and time the incident occurred	
Date and time the school became aware of the incident	
How did you first become aware of the incident? (e.g. reported by a staff member, parent or pupil)	
Who has the incident been reported to? (name and position at the school, or external organisations such as your IT team or the police)	
Incident reference number (if applicable for your school)	
Description of the incident Please provide as much detail and write as clearly as possible, including: • Who was involved and advised (job titles) • The cause of the breach (e.g. high workload, distracting workspace, new system, lack of training) • Explanation of any delay in reporting the incident	
Initial response by the school Provide details of any immediate actions that you have taken (e.g. removed published data, requested deletion of an email, password changes on systems, theft of equipment reported to the police).	
Have you been able to recover the personal data (if applicable)? Provide details e.g. you have retrieved a letter sent to the wrong parent etc.	
Have you informed the data subject(s)?	

Part 1 - About the incident	
This is the person the information relates to. If you have informed them please briefly describe their reaction (e.g. are they very concerned? Did they express any particular worries?).	

Part 2 – About the personal data	
How many individuals did the breached data relate to?	
Are there other people who may also be affected by the breach of the personal data? If so, how many? (E.g. parents of the pupils, family of a teacher etc.?)	
Categories of individuals affected Select all that apply	Employees ☐ Pupils ☐ Parents ☐ Other (please give details below): ☐ Click or tap here to enter text.
Does the information disclosed contain data that could identify the individuals? Select all those that apply	Name ☐ DOB ☐ Contact details ☐ Location data ☐ Online identifiers such as IP address and cookie identifiers ☐ Identification data such as usernames or passwords ☐ Official documents (e.g. passport) ☐ Free school meal status ☐ Other (please give details below): ☐ Click or tap here to enter text.
Does the data contain any sensitive or special category data? Select all that apply	Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Genetic data ☐ Biometric data ☐ Health data (including SEN info) ☐ Data regarding sex life or orientation ☐ Criminal offence data ☐ Safeguarding information ☐ Financial information (bank details, credit card numbers, any information indicating financial status) ☐
Are there any other details which should be noted? e.g. any additional risks which could increase the harm/detriment to individuals	

Part 2 – About the personal data	
involved or affect the investigation in any way.	

Stage 2: Risk assessment scoring

Please use the risk matrix scoring form (appendix one of Data Breach Policy) and add the score and risk level to the box below.

Risk Score from Matrix (totals from all tables)	

Decision to inform data subjects/individuals affected

Reportable to individuals from the Matrix? Please select.	**NO**
Are there additional factors to consider regarding notifying individuals? Provide your reasoning and if specialist advice was required.	
Final decision to inform	Choose an item.
Decision makers details	
Date	Click or tap to enter a date.

Decision to inform ICO (made in conjunction with the DPO)

Reportable to ICO from the matrix? Please select.	**NO**
Are there additional factors to consider regarding notification? Provide your reasoning and if specialist advice was required.	
Final decision to inform	Choose an item.
Decision makers details	
Date	Click or tap to enter a date.
DPO details	
Date	Click or tap to enter a date.

Stage 3: Investigation

Understanding what data security measures are currently in place This section is about the internal controls that the school has in place to protect all data it holds across its systems, both electronically and physical files.

Provide details of any relevant measures you already had in place to prevent a breach of this type occurring. For example: • Details of staff training, • What policies , processes and procedures are used within the school • Security controls in place (both physical – locked storage etc. and technical – passwords, encryption etc.).	
Are there relevant policies, procedures or guidance that set out what should have happened. If so what are they?	
Were the above appropriate security guidelines being followed? If not explain why.	
Has this type of incident occurred at the school before? If so, provide please a brief summary of • The date when it happened, • Who was involved in the incident (job titles) What the outcome of the investigation was (E.g. was any additional security or training put in place?)	

Training and communication This section is about whether staff understood what organisational and technical data security measures were in place	
If a member of staff was involved in the personal data breach, have they received data protection training within the last two years? (Please confirm what training has been completed)	
What evidence is there to communicate the process to be followed? (E.g. email reminders or staff meeting discussions)	
Was the training/communications provided being followed? If not explain why.	

Other factors for consideration	
Please provide any other factors that should be taken into consideration relating to the security incident. (E.g. the use of autocomplete for email addresses meant the wrong email address was selected)	

What was the root cause? (E.g. a change in working conditions, working from home, higher workload, staff absence, a lack of appropriate equipment, technology issues, lack of secure storage)	