Healthy Empowered Ambitious Respectful Together

Our values are at the HEART of our school

Data Breach Policy

Policy Author:	Alison Hall
Date of Policy Review:	September 2024
Date approved by Governors:	November 2024
Next Review Date:	November 2026

1.0 Introduction

1.1 Washingwell Community Primary School 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 protection 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.

2.0 Purpose

2.1 Washingwell Primary School is obliged under the Data Protection Act and the General Data Protection Regulation to:

2.2 have in place a framework designed to ensure security of all personal data during its lifecycle, including clear lines of responsibility.

2.3 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 school.

3.0 **Scope**

3.1 This policy relates to all personal and special category data held by the school regardless of format.

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

3.3 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**

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

4.2 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 school's information assets and/or reputation.

4.3 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, I Pad/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.

5.0 Reporting an incident

5.1 Any individual who accesses, uses or manages the School's data is responsible for reporting the data breach and information security incidents immediately to infosecurity@washingwell.org.uk

5.2 The school will inform the Data Protection Officer

5.3 If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. Note: The school only has 72 hours to report a breach to the Information Commissioner.

5.4 The report will 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, and how many people are involved. An incident reporting form should be completed as part of the reporting process. See Appendix 1

6.0 Containment and recovery

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

6.2 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 (this will depend on the nature of the breach, in some cases it could be the DPO)

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

6.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the Police, where appropriate.

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

7.0 Investigation and Risk Assessment

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

7.2 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.

7.3 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

8.0 Notification

8.1 The LIO and/or the DPO, in consultation with the Head Teacher, will determine whether the breach needs to be reported to the Information Commissioner.

8.2 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 – 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 school/academy meet its obligation sunder the principle
- Whether this breach constitutes a high risk to individuals and therefore needs to be reported to the ICO

8.3 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 school/academy for further information or to ask questions about what has occurred.

8.4 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.

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

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

9.0 Evaluation and response

9.1 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.

9.2 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.

9.3 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 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 your Head Teacher of it immediately and report it via inforsecurity@washingwell.org.uk and inform SchoolsDPO@veritau.co.uk

Section 1: Notification of Data Security Breach	**To be completed by Head Teacher reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head Teacher if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the School/Academy or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • Special Category data (as defined in the Data Protection Act) relating to a living, identifiable individual's a) Racial or ethnic origin; b) Political opinions or religious or philosophical beliefs; c) Membership of a trade union; d) Physical or mental health or condition or sexual life; e) Biometric data	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to parents, staff and children	
• Detailed profiles of individuals including information about work performance,	

salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals	
• Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	**To be completed by Data Protection Officer and/or Lead Investigation Officer**
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**