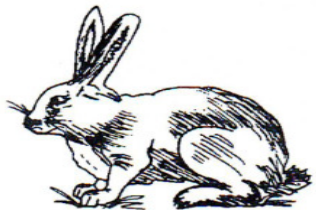

Harefield Junior School
Data Breach Policy

May 2018

Introduction
Harefield Junior School holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected.

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

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

Purpose
Harefield Junior School is obliged under the Data Protection Act to have in place an institutional 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 breach and information security incidents across the school.

Scope
This Policy relates to all personal and sensitive data held by the school regardless of format.

The Policy applies to all staff at the school. This includes temporary, casual or agency staff and contractors, consultants, 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 action is necessary to secure personal data and prevent further breaches.

Definition/Types of Breach
For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this Policy is an event or action 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.

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

- Loss or theft or confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, 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 IT system(s).
- Unauthorised disclosure of sensitive/confidential data.
- Website defacement.
- Hacking attack.
- Unforseen circumstances such as a fire or flood.
- Human error.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an Incident

Any individual who accesses, uses or manages the school's information is responsible for reporting data breach and information security incidents immediately to their line manager. In the case of the Head of School the Executive Head teacher and in the case of the Executive Head teacher the Chair of Governors.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

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 individuals are involved. An Incident Report Form should be completed as part of the reporting process. See Appendix 1.

All staff should be aware that any breach of the Data Protection Act may result in the school's disciplinary procedures being instigated.

Containment and Recovery

The investigation 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.

An initial assessment will be made by the investigation 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).

The lead investigator will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The lead investigator will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts may be sought in resolving the incident promptly.

The lead investigator, in liaison with relevant staff, will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and Risk Assessment
An investigation will be undertaken by the lead investigator immediately and wherever possible within 24 hours of the breach being discovered/reported.

The lead investigator will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences 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.
- Its sensitivity
- The protections are in place (e.g. encryptions)
- What's happened to the data, has it been lost or stolen
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- Whether there are wider consequences to the break.

Notification
The lead investigator, in consultation with the Head of School, Executive Head teacher or Chair of Governors, will determine who needs to be notified of the breach.

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 the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Would notification help the school meet its obligation under the seventh data protection principle?
- If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Officer (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify the ICO is available from their website at https://ico.org.uk/media/1536/breach_reporting.pdf
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

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 for further information or to ask questions on what has occurred.

The lead investigator and The Governing Body 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.

The lead investigator and/or the will consider whether The Local Authority should be informed regarding a press release and to be ready to handle any incoming press enquiries.

All actions will be recorded by the lead investigator.

Evaluation and Response
Once the initial incident is contained, the Governing Body will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and 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 personal data is held and where and how it is stored.
Where the biggest risks lie, and will identify any further potential weak points within its existing measure.
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.

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by The Governing Body

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify The Head of School, Executive Head teacher or the Chair of Governors immediately, and complete Section 1 of this form.

Section 1: Notification of Data Security Breach	To be completed by person reporting incident
Date incident 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 INSERT DETAILS HERE	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigator in consultation with appropriate staff 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, financial legal, liability or reputational consequences for the school 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 • Sensitive personal 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) Commission or alleged commission of any offence, or f) Proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
• 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 vulnerable adults 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 pupils, information about individual cases of pupil discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	
Lead Investigator to consider whether it should be escalated to The Chair of Governors	

Section 3: Action Taken	To be completed Lead Investigator
Incident number:	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Contact details of person reporting incident (email address, telephone number):	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to INSERT NAME HERE/Lead Investigator on (date):	
Reported to other internal stakeholders (details, dates):	
For use of INSERT NAME HERE / Lead Investigator:	
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:**

Date of next review: May 2020