Halley Primary School
Including all learners and achieving great things

Halley Primary School
Data Security Breach Policy

Document Control		
Draft Issued	May 2018	
Author	Lisa Payne	School Business Manager
Draft Approval	Wendy Otterburn-Hall	Head Teacher
Signed off by	Governing Body 27th June Chair: Lissa Samuel	
Review Date	June 2020	
Review Cycle	Biennial	

Data Breach Policy

What is a data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party, hacking;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices (USB, laptops, tablets) containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data

A personal data breach can be defined as a **security incident** that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If a Personal data breaches has occurred

There are four important elements when dealing with a data:

1) Containment and recovery
2) Assessment of ongoing risk
3) Notification/reporting of breach
4) Evaluation and response

1) Containment & recovery

Report any breach or possible breach to the school's Data Protection Officer (DPO). Our DPO is **Louise Manthorpe** and is contactable via details below:

LBTH Schools DPO

school.dpo@towerhamlets.gov.uk
020 7364 6570

If the DPO is unavailable all breaches must be reported to the School Business Manager or Head.

- The DPO will lead on the investigation and depending on the breach will act. Examples of actions are to: try & locate lost item, isolate part of the network, changing passwords, resetting access codes to doors, informing police if necessary & making any 3rd parties aware. A detailed record of how the breach was managed should be kept on the "Incident Time Line Activity Record" (Appendix A)

2) Assessing the Risk

- The DPO will assess the risk of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.
- They will use the following points: (See Appendix B)

  - What is the nature of the breach?
  - What type of data is involved?
  - How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
  - If data has been lost or stolen, are there any protections in place such as encryption?
  - What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
  - Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of a person's identity.

3. Notification of a Breach

- The DPO will assess the breach to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then they will notify the ICO; if it's unlikely then they won't have to report it. However, if it isn't reported, they will need to be able to justify this decision, so it should be documented on Breach Risk Assessment Checklist (Appendix B).
- If impact is high the DPO will report the breach to the ICO by either calling:

ICO - 0303 123 1113

And informing them of

- what has happened;
- when and how you found out about the breach;
- the people that have been or may be affected by the breach;
- what you are doing as a result of the breach; and
- who we should contact if we need more information and who else you have told

Or by completing a data breach notification form (Appendix C)

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, DPO must also inform those individuals without undue delay.
- All breaches must be added to the Data LOG

Effects of a Data Breach

A breach can have a range of adverse effects on individuals, which include:

- ➢ emotional distress
- ➢ physical damage and
- ➢ material damage

Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

Appendix

A - Incident Time Line Activity Record

B - Breach Risk Assessment Checklist

C - ICO Breach Notification Form

APPENDIX A - Incident Time Line Activity Record

DATE/TIME	ACTIVITY	ACTION	OWNER	COMPLETED
25/05/2018 *9.30AM*	*Received notification personal data in on the website*	*Informed web team & immediately asked them to take down*	*L.Payne*	*13.00*

APPENDIX B : SECURITY BREACH RISK ASSESSMENT CHECKLIST

a) What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)

b) How did the breach occur?

c) What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)

d) How many individuals or records are involved?

e) If the breach involved personal data, who are the individuals? (Pupils, staff, parents, etc)?

f) What has happened to the data?

g) Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)

h) Were there any protections in place? (e.g. Encryption)

i) What are the potential adverse consequences for individuals or the University? How serious or substantial are they and how likely are they to occur?

j) What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?

k) What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted)

Data protection breach notification form

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. Organisation details

(a) * What is the name of your organisation – is it the data controller in respect of this breach?

(b) Please provide the data controller's registration number. Search the online Data Protection Public Register.

(c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

2. Details of the data protection breach

(a) * Please describe the incident in as much detail as possible.

(b) * When did the incident happen?

(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Personal data placed at risk

(a) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse
effects on those individuals?

(e) Have any affected individuals complained to the organisation about the incident?

4. Containment and recovery

(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has your organisation taken to prevent a recurrence of this incident?

5. Training and guidance

(a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

Sending this form

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on
0303 123 1113 or **01625 545745** (operates 9am to 5pm Monday to Friday)