First version: May 2018
Revision 1.3: 14/09/18

Data Protection - Data Breach Procedure

Procedure Statement

To meet its public duty and legal obligations, Hook Infant School collects, uses and stores large amounts of personal and sensitive data. Although every care is taken to protect this data it is important to recognise that human error, system faults and inappropriate or malicious activity can result in a data breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

This procedure sets out the course of action to be followed by all staff if a data protection breach takes place. For the purpose of clarity, all suppliers or contractors will be referred to as 'processors'.

Legal Context

Article 4 (12) of the General data protection Regulation (GDPR) defines a data breach as:

"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Hook Infant School is obliged under the GDPR to act in respect of such data breaches.

Excerpt: *Article 33 of the General Data Protection Regulations*
Notification of a personal data breach to the supervisory authority

1. *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

2. *The processor shall notify the controller without undue delay after becoming aware of a personal data breach.*

3. *The notification referred to in paragraph 1 shall at least:*
   - *(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*
   - *(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
   - *(c) describe the likely consequences of the personal data breach;*
   - *(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

4. *Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

5. *The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.*

Managing a Data Breach

In the event that a member of staff or Governing body identifies or is notified of a personal data breach, the following steps should followed to contain the breach:

1. The person who discovers/receives a report of a breach must inform the Headteacher and/or the School's Data Protection Officer (DPO), in their absence the Deputy Head or other member of the Senior Leadership Team should be notified. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff or processors.

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors and Data Protection Governor as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct the investigation of the breach.

4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. 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. In such instances, advice from the School's legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    - taking affected devices or services offline or cease to process until further notice;
    - contacting third parties or other unauthorised individuals who may have received personal data in error, such as an email sent in error will be contacted and requested that they delete all data and confirm in writing that this has been completed;
    - contacting processors to gather evidence of the breach and determine the impact on data and data subjects.
    - Attempting to recover lost equipment.
    - Contacting Hampshire Legal Services and Children's Services, so that they can be prepared to handle any press enquiries. See contacts at end of this document.
    - The use of back-ups to restore lost/damaged/stolen data.

- If finance details have been lost or stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher/DPO (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (or nominated representative) should establish the extent of the data involved, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- The level of sensitivity or confidentiality;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Details of who has seen or received the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be conducted once the matter has been resolved.

Notification

As part of the investigation, individuals, third parties or processors may need to be notified as part of the containment in order to recall data, request deletion or to perform other actions.

In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. It is advisable that Hampshire Legal and/or Children's Services should be notified in these instances. The Head Teacher/DPO (or nominated representative) should, after seeking expert or legal advice, review whether affected data subjects are notified of the breach.

If the breach is likely to result in a "**high risk to the rights and freedoms**" of affected data subjects, they must be notified of incident, the school's actions and offered support and advice.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred, what data was involved and details of what has been done to mitigate the risks posed by the breach.

Review and Evaluation

When the breach has been brought under control, the Head Teacher/DPO (or nominated representative) should fully review the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leadership Team and Full Governing Body meeting for discussion. If the breach warrants a disciplinary investigation, the Headteacher should liaise with Hampshire Legal and Personnel for advice and guidance.

This breach procedure may need to be reviewed following a data breach or after legislative changes, or following new guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements, including this data breach procedure. This should be undertaken as part of induction, supervision and ongoing training.

Contacts

If you have any queries in relation to this procedure please contact the school's Data Protection Officer who will act as the contact point for any data protection matters.

Data Protection Officer:	Peter West Hook Infant School Church View, Hook Hampshire. RG27 9NR
Telephone:	01256 764487
Email:	p.west@hook-inf.hants.sch.uk

Alternatively, you can also discuss this with your line manager or the Headteacher.

Contact details for Local Authority Departments:

Hampshire Legal Services

Hampshire County Council

The Castle

Winchester

SO23 8UJ

01962 847378

Data Breach Notification Flowchart