Data Protection - Data Breach Procedure for Broomfield School

Policy Statement

Broomfield School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection 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 applies to all personal and sensitive data held by Broomfield School and all school staff, Advisory Board Members, volunteers and contractors, collectively called staff for the purposes of this procedure.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Broomfield School if a data protection breach takes place.

Legal Context

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.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or Proprietor's data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Unforeseen circumstances, such as a fire or flood;
- Unauthorised disclosure of sensitive/confidential data;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the school identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Headteacher and the School's Data Protection Officer (DPO) using the form attached to this procedure. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Headteacher/DPO 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 such as the IT team.
3. The Headteacher/DPO must inform the Proprietor and School Advisory Board as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.
4. The Headteacher/DPO 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 HCC legal team should be sought.
5. The Headteacher/DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
   a. Attempting to recover lost equipment.
   b. Contacting all school staff so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Headteacher/DPO.
   c. Contacting the School's IT consultants for their advice and help in overcoming any problems caused by this breach.
   d. The use of back-ups to restore lost/damaged/stolen data.
   e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
   f. 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 will be for the Headteacher/DPO to fully investigate the breach. The Headteacher/DPO should ascertain whose data was involved in the breach, 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;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to 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 any wider consequences to the breach.

A clear record, using the form attached to this procedure, should be made of the nature of the breach, the investigation, the actions taken to mitigate it and the reports made to authorities concerning the breach. 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 done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision to notify will normally be made once an initial investigation has taken place. The Headteacher/DPO should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

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 Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Headteacher/DPO should fully review both the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Education Personnel Services and HCC Legal for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

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 potential weak points within its existing security measures;
- whether methods of transmission are secure (sharing minimum amount of data necessary);
- staff awareness (liaising with HR Officer to inform future staff training where appropriate); and
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If appropriate, the DPO will recommend any changes to systems, policies and procedures to the Senior Leadership Team and Board of Directors.

Implementation

The Headteacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the school's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Headteacher.

Broomfield School
DATA BREACH REPORTING FORM

The aim of this document is to ensure that, in the event of a security incident such as personal data loss, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.
The checklist can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer (School Business Manager) who can determine the implications for the school, assess whether changes are required to existing processes and notify the ICO / data subject where appropriate.

SUMMARY OF INCIDENT	
Data and time of incident	
Nature of breach (e.g. theft/ disclosed in error/ technical problems)	
Give a full description of how breach occurred	
PERSONAL DATA	
Give a full description of all the types of personal data involved with the breach but not specifically identifying the individual concerned (e.g. name, addresses, health information etc.)	
How many individuals are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further disclosed? If so, please provide details	
IMPACT OF INCIDENT	

What harm is foreseen to the individuals affected? (e.g. could the breach increase the risk of identity theft?)	
What measures have been taken to minimise the impact of the incident?	
Has the data been retrieved or deleted? If yes, state when and how	
REPORTING	
Who became aware of the breach?	
How did they become aware of the breach?	
Form Completed by	
Position	
Date	