Appendix 5: Data Breach Procedure Henbury View First School

About this procedure

This procedure describes the actions that must be taken by staff to report any incident which may result in a personal data breach. A "personal data breach" is defined in Article 4(12) of the General Data Protection Regulation as:

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

Often, when an incident first comes to light, it will not be possible to determine whether or not it constitutes a personal data breach. The term "incident" is used in this policy to describe any situation which may, upon investigation, turn out to be a personal data breach.

1. Identifying an incident

An incident may come to light in a number of ways. For example, it could occur by:

- direct observation e.g. where a member of staff spots that personal data has been sent to the wrong email address;
- being reported to us by a pupil or parent: e.g. where a pupil notifies us that she/he has received personal data relating to another pupil;
- being reported to us by another party, such as a contractor, a local authority or a member of the public; or
- an audit / review revealing that an incident had occurred.

2. Actions to take once an incident has been identified

Whenever an incident is identified, the following actions must be taken:

	Action	Responsibility	Timelines
1.	Report the incident to the Data Compliance Officer Mrs Claire Elms	Member of staff who was first made aware of the incident	**Immediately after the incident is identified**
2.	Investigate and identify the full details of the incident to identify the cause	Data Compliance Officer for the school (with the assistance of the colleague	**As soon as possible following the incident being reported**

		who reported the incident)	
3.	Identify any remedial action (see section 4, below)	Data Compliance Officer for the school	**As soon as possible following the incident being reported**
4.	Complete a formal Personal Data Breach Form and return it to Data Protection Officer	Data Protection officer	**Within 48 hours of the incident being identified**
5.	Review the Personal Data Breach Form and determine whether the incident constitutes a personal data breach or a 'near miss' (i.e. an incident which does not meet the definition of a personal data breach)	Data Protection Officer (in conjunction with the Data Compliance Officer for the school)	**As soon as possible following step 4**
6.	If necessary, decide whether to notify (i) the ICO; and/or (ii) individual data subjects, of the personal data breach (see section 5, below)	Data Protection Officer (in conjunction with the Data Compliance Officer for the school)	**As soon as possible following step 4**
7.	If necessary, notify the ICO of the personal data breach	Data Protection Officer	**Within 72 hours of the incident being identified**
8.	If necessary, notify individual data subjects of the personal data breach	Data Protection Officer	**Without undue delay (in practice this should be done as soon as possible)**

3. Taking remedial action

Following the reporting of the issue, the school's Data Protection Officer shall advise the relevant Data Compliance Officer what remedial action must be taken, in particular where pupils or parents are affected in any way by the personal data breach. Pupils or parents may suffer distress and inconvenience where they are aware that a breach has occurred. In some cases, they may be at risk of suffering financial detriment or physical harm as a result of the breach.

Remedial action should seek to mitigate any risks the pupil or parent has been exposed to as a result of the breach, to prevent similar breaches occurring in the future and to protect the school. Action will be dependent on case specifics, but the Data Protection Officer should consider the school's responsibility to act in the best interests of pupils and parents.

If there is any doubt at all about the remedial action required to be taken, the Data Compliance Officer will consult the school's governing body

Remedial action might include the following:

- If personal data is in the hands of a third party, it should be retrieved from the third party
- If the breach arose as a result of an IT issue, the source of the issue should be identified and rectified .
- If the breach arose as a result of human error, the individual should be made aware of the error and where appropriate asked to undertake additional training or (only in the most serious cases) be subjected to disciplinary action.

4. Notifying a personal data breach

Under the General Data Protection Regulation, there is an obligation to report a personal data breach to the Information Commissioner's Office (ICO) 'without undue delay' and in any event within 72 hours of us becoming aware of the breach.

There is an exception to this reporting requirement where the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected. A decision on whether the breach must be reported to the ICO will be made by the Henbury View First School's Data Protection Officer following receipt of the Personal Data Breach Form.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals affected, there is an obligation to notify those individuals of the breach 'without undue delay'. A personal data breach that may result in a high risk to individuals may include where a parent is exposed to the risk of suffering financial detriment or physical harm if they are not notified of the breach. Where this is the case, then Henbury View First School's Data Protection Officer must inform them of the breach by letter and make a formal apology. Henbury View First School's Data Protection Officer will make the final decision as to whether notifying individuals is required.

Where pupils or parents are aware that they are the subject of a personal data breach, then they must be issued with a written apology. Brief details of the remedial action taken should be provided to reassure them, where this information can be provided without revealing any personal or confidential information.

Where appropriate, remedial action should also consider anyone other than the pupil(s) or parent(s) who may also have been affected indirectly. These individuals should also be sent a written apology to minimise the Henbury View First School's reputational damage.

As well as the requirement to report personal data breaches to the ICO, it may also be necessary to report them to other authorities such as the police. These actions should only be undertaken following consultation with Henbury View First School's Data Protection Officer.

5. Follow-up action

To ensure that we learn from our mistakes, the school is required not only to confirm that remedial action has taken place, but also that the causes of the personal data breach have been analysed and action taken to ensure similar breaches do not occur again. Confirmation of this action is reported and saved by Henbury View First School's Data Protection Officer as an audit trail.

6. Central logging of the issue

Once the school has confirmed remedial action and any appropriate follow-up action, then, subject to:

- the pupil(s) or parent(s) being satisfied with the remedial action taken in respect of the breach and;
- the Data Protection Officer being satisfied that regulatory procedures have been followed,

then the breach can be marked as closed by the Data Protection Officer.

A copy of all breach forms will be kept by the Data Protection Officer and stored in the Head's Office.