Highwood Primary School

"Preparing today's children
for tomorrow's world"

Data Security Breach Management Policy

Written September 2014
Review date September 2018
Ratified by Governors

The Data Protection Act 1998 (DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

Overview

This policy sets out some of the things that the school will consider in the event of a security breach in order that an appropriate course of action is taken.

As Highwood processes personal data, the school must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

Definition

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 transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service."

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Action

However the breach has occurred, there are four important elements to any breach management plan:

1.Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation.(See Appendix 1) This will often involve input from specialists such as IT, HR and legal and in some cases contact with external stakeholders.

Should a data breach occur at Highwood, the Headteacher, in conjunction with the Senior Leadership team will:

- Take the lead on investigating the breach, ensuring that appropriate resources are available.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.

- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police.

2. Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered. Before deciding on what steps are necessary, we will assess the risks which may be associated with the breach. We will carry out an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. To do this, we will consider the following points:

- What type of data is involved?
- How sensitive is it?
- 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, could it be used for purposes which are harmful to the individuals to whom the data relate?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?

3. Notification of breaches

Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

When deciding whether a breach requires informing people or organisations, the following will be considered:

- Are there any legal or contractual requirements?
- Can notification help meet the schools security obligations whereby appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, you should inform the ICO.
- How can notification be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

The Headteacher, in conjunction with the Senior Leadership Team will consider who to notify, what they will be told and how the message will be communicated. This will depend to a large

extent on the nature of the breach but the following points will be considered when making decisions:

- If a data breach occurs, the school will inform the Chair or Governors
- Contact will be made with the Chief Data Protection Manager at County. Depending on the level of the breach, they may then require the school to notify the ICO.
- Any notification will at the very least include a description of how and when the breach occurred and what data was involved. Data breaches will be recorded in the data breach log (See Appendix 1) Details of what the school has already done to respond to the risks posed by the breach should also be included.
- When notifying individuals specific and clear advice will be given on the steps they can take to protect themselves and also what the school can do to help them

Should the data breach be reported to the ICO, details of the security measures in place such as encryption and, where appropriate, details of the security procedures the school had in place at the time the breach occurred will be included. If the media become aware of the breach, the ICO will also be notified so that they can support the school in managing enquiries.

4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the school's response to it. Following any breach, the school will identify where improvements to data protection procedures can be made. The school will:

- Review what personal data is held and where and how it is stored.
- Establish where the biggest risks lie and ensure that appropriate measures are in place to minimise the risk of further security breaches.
- Ensure that not only is the method of transmission secure but also that the school only shares or discloses the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in the existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.

Any data security breaches will be recorded in the data security breach log (Appendix 1)
This log will be shared with Governors annually.

Policy Written: September 2014
Review: September 2016

Appendix 1 – Personal Data Security Breach Log

Organisation:	Date:

No.	Your ref.	Details of breach						Consequences of breach	Measures taken/to be taken			
		Date of breach	No. people affected	Nature of breach (choose most relevant)	Description of breach	How you became aware of breach	Description of data		All individuals informed?	Remedial action	Other Regulators informed	When did you first notify the ICO of the breach?