Brook Community Primary School
Data security breach management policy and procedures

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.

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." 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 our breach management plan:

1. <u>Containment and recovery</u>
   Should a data breach occur, the Headteacher 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 limiting access to certain parts of the school.
   - 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 ensuring that staff recognise when someone tries to use stolen data to access accounts.
   - Where appropriate, inform the police.

2. <u>Assessing the risks</u>
   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 that 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 that are harmful to the individuals to whom the data relates?
- 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?

3. <u>Notification of breaches</u>

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 other people or organisations, the following will be considered:

- Are there any legal or contractual obligations?
- Can notification help meet the school's 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, we are aware of our duty to inform the Information Commissioner's Office (ICO).
- How can notification be made appropriate for particular groups of individuals, for example, if we are notifying children?

The Headteacher 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 Headteacher will always inform the Chair of Governors and Data Protection Officer.
- Depending on the severity of the breach, contact will be made with the Records Manager for Kent County Council. 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.
- 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. <u>Evaluation and response</u>
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 transition 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.
    - Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.