Believe in Yourself

Whitehouse Primary School

Data Breach Process

This policy outlines what the school will consider in the event of a data breach in order that the most appropriate course of action is taken.

Definition

A personal data breach is;

> *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data."*

A data 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
- Actos of God such as fire and flood
- An external hacking attack
- An organisation receiving information by deception

However the breach has occurred there are four elements to our breach management plan.

Actions

1. **Containment and recovery.** Should a breach occur, the DPO will:
    - Take the lead on investigating the breach, ensuring that appropriate resources are available.
    - Identify who needs to be made aware of the breach and inform them of what they are expected to do to assist in the clear-up including finding lost equipment or limiting access to certain parts of the school or the network.
    - Establish whether they is any chance of recovering any losses and limiting the damage the breach has caused.
    - Whether or not the police and ICO need to be informed.

2. **Assessing the risks.** Some data breaches will not lead to risks beyond an inconvenience to those that need the data to do their job. For example a laptop could be irreparably damaged but the files will be backed up and can be recovered. We will carry out an assessment of potential adverse consequences for individuals, how serious or substantial these are and, how likely are these to happen. To do this, we will look at the following:
    - What type of data was involved?
    - The sensitivity of the data?
    - Was the data protected by encryption?
    - What has happened to the data; if it has been stolen could it be used for purposes that are harmful to the individual data subjects?
    - What could the data tell a third party about the data subject?
    - How many data subjects are involved in the breach?

- Who are the data subjects?
- What harm could the breach cause these individuals i.e. is there a risk to life or financial loss or both?
- Are there any wider consequences?

3. **Notification of Breaches.** All notifications should have a clear purpose whether this is to enable individuals who may have affected and to allow the ICO to investigate in line with legal obligations. When deciding if a breach needs to be reported we will consider:
    - Any legal or contractual obligations.
    - Can notification help the individual bearing in mind the potential effects of the breach.
    - How can we make the notification appropriate for the data subjects involved e.g. children.
    - Our obligations under the General Data Protection Regulations 2018 and the need to notify the ICO within 72 hours of a breach.

The DPO will consider who to notify, what they will be told and how the message will be communicated. The notification will ensure that data subjects are advised how to protect themselves and what more the school can do to help.

The DPO will also advise the Chair of Governors, North Tyneside Council and North Tyneside Learning Trust IT teams to consider further action or additional reporting to the ICO depending on the nature of the breach.

4. **Evaluation and response.** A key aspect of investigating any breach is to ensure that the school can learn lessons and ensure the risks of further breach are minimised. Following the immediate breach containment actions the school will:

    - Review what personal data is held and where and how it is stored.
    - Identify the biggest risks in the process and see what can be done to minimise these.
    - Ensure that the school only shares the minimum amount of data and that sharing of data is as secure as possible.
    - Identify weak points in the systems and what the school can do to minimise these.
    - Ensure that staff are reminded of their obligations to ensure the safety of personal data.
    - Take appropriate action if the data breach was a deliberate act by a member of staff.

This policy will be reviewed on a two yearly cycle or when a breach occurs. The next review will be March 2020.