Data Breach Policy
September 2023

Introduction

Pele Trust is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the Trust and its schools are protected.

The Trust recognises, however, that any organisation can be subject to breaches of security particularly given the amount of information that is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks.

What is a personal data breach?

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.

This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

Identifying a personal data breach

Any member of staff who becomes aware of a personal data breach, or is concerned that a personal data breach may have occurred, should report it to the school Headteacher or Business Manager immediately.

Failure to do so may prevent the timely containment of the breach and result in the school falling foul of GDPR requirements.

The priority in the first instance will always be to assess the risk of any breach in order to take the most appropriate action.

Recording a breach

When an incident is raised the Headteacher or nominated colleague will gather and record the following information:

- Name of the individual who has raised the incident
- Description of the incident
- Description of the data which may be compromised
- Description of any perceived impact
- Description of any devices involved, e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident

All breaches will be recorded in the Data Breach Log which is held by the Chief Operating Officer.

Assessing the risk

As quickly as reasonably possible it should be determined whether any personal data is involved or compromised and if so, to what extent and severity.

The investigation officer will consider the impact of the breach in terms of likelihood and severity of the resulting risk to people's rights and freedoms.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

The following questions will be considered in order to fully and effectively assess the risks that the breach has brought, and to help take the next appropriate steps.

- What type and how much data is involved?
- How sensitive is the data (as defined in the GDPR)?
- Has individuals' personal data been compromised – how many individuals are affected?

- Who are these individuals – are they pupils, staff, Academy Committee Members, volunteers, stakeholders, suppliers?

- Could their information be misused or manipulated in any way?

- Could harm come to individuals? This could include risks to the following:
    - Physical safety
    - Emotional wellbeing
    - Reputation
    - Finances
    - Identity
    - Private affairs becoming public

- What has happened to the data – has it been lost, stolen, deleted or tampered with?
- Are there any protective measures in place to prevent or restrict access to the data such as data and/or device encryption?
- If the data has been compromised are effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?

- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?

In the event that the person assessing the risks to the school are not confident in the risk assessment they will seek advice from the Trust Data Protection Officer and/or the Information Commissioner's Office (ICO).

Low Risk Breach

If it is the determined that the severity and associated risk of the data breach is low, the incident will be managed in accordance with the following procedures:

- The incident is recorded using the Data Breach log log.
- All necessary action will be taken to minimise the breach and prevent any recurrence.
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.
- Training and guidance will be provided for any individual concerned.

High Risk Breach

Where the breach is significant, or the impact or risk is high the school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Reporting the breach to the Trust Data Protection Officer
- Reporting the breach to the ICO
- Notifying affected individuals of the breach
- Informing relevant staff of their roles and responsibilities in areas of the containment process
- Taking systems offline
- Retrieving any lost, stolen or otherwise unaccounted for data
- Restricting access to systems entirely or to a small group
- Backing up all existing data and storing it in a safe location
- Reviewing basic security, including:
    - Changing passwords and login details on electronic equipment.
    - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the Headteacher will inform the police of the data breach.

Reporting a breach to the ICO

A serious breach must be reported to the ICO at the earliest possible opportunity but certainly within 72 hours of the school becoming aware of the breach.

When reporting a breach the GDPR requires that the following information be provided:

- A description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- The name and contact details of the school data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

It is possible that not all information will be available without further or additional investigation. This should not prevent the incident being reported to the ICO. There is provision within the GDPR to provide information in stages as long as appropriate priority is being given to the investigation.

Consideration of further notification

The Trust will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security.

Monitoring and review

Breaches will be reviewed by the Headteacher and Trust Data Protection Officer on a regular basis to ensure the effectiveness of this policy and data protection policies in school.