PINNER WOOD SCHOOL

DATA SECURITY BREACH POLICY

Approval Authority:	
Effective From:	September 2023
Date Ratified by GB:	
Next Review Date:	September 2024
Signed by Chair of GB:	

Data Security Breach Policy

This policy is for information on what to do in the event of a personal data information security breach. It sets out what we need to consider in the event of a breach including, containment/recovery, course of action, risks, reporting and evaluation and response.

Overview

As a school we process personal data so we must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

A personal 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 school/employees

It is the duty of the DPO or designated person to complete the Breach Management Plan if a breach occurs. Please see Breach Management Plan for further details.

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. It also means that a breach is more than just about losing personal data.

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.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Types of breach

Breaches can be categorised according to the following three well-known information security principles:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

A breach can include but is not limited to:

- Loss/theft of a personal device where school emails/data is accessed
- Loss of a memory stick
- Email containing personal data sent to the wrong recipient
- Accidentally/unintentionally clicking on a 'Phishing' link within an email

What to do if you identify a breach

All staff are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

You must notify your line manager as well as the Data Protection Officer on: dpo@pinnerwood.co.uk

You must give as much detail as possible about the breach including your name, department and date and time that the breach was identified.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so we need to document it in GDPRiS.

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."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. We need to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, we should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

We should ensure that you record all breaches in GDPRiS, regardless of whether or not they need to be reported to the ICO.

How much time do we have to report a breach?

We must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have 'become aware' of a breach.

What information must a breach notification to the supervisory authority contain?

When reporting a breach we must provide:

- 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 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.

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows us to provide the required information in phases, as long as this is done without undue further delay.

However, the ICO expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. We must still notify the ICO of the breach when we become aware of it, and submit further information as soon as possible. If we know we won't be able to provide full details within 72 hours, it is a good idea to explain the delay to the ICO and tell them when we expect to submit more information.

How to notify a breach to the ICO

The DPO will report any breaches to The ICO via their breach reporting tool online. The DPO will use the link below to report a breach.

https://ico.org.uk/for-organisations/report-a-breach

When to tell individuals about a breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. We will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, we will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If we decide not to notify individuals, we will still need to notify the ICO unless we can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. We should also remember that the ICO has the power to compel us to inform affected individuals if they consider there is a high risk. In any event, we should document your decision-making process in line with the requirements of the accountability principle.

Information we must provide to individuals when telling them about a breach

We need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of our 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 and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of turnover. The fine can be combined by the ICO's other corrective powers under Article 58.