GDPR 2018 Data Breach Notification Procedure – Pinnacle Learning Trust

Data Breach Notification Procedure

This procedure applies in the event of a personal data breach under Article 33, 'Notification of a personal data breach to the supervisory authority', and Article 34, 'Communication of a personal data breach to the data subject of the GDPR.' We have 72 hours from notification of data breach to investigate and act.

Responsibility

All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) of The Pinnacle Learning Trust are required to be aware of, and to follow this procedure in the event of a personal data breach.

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. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

Example

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.

Incidents include:

- password disclosure
- loss / theft / disclosure of confidential or sensitive electronic data / emails
- loss / theft / disclosure of confidential or sensitive written data / faxes / photocopies
- virus warnings / alerts on work PC
- loss / theft of equipment such as laptops, USBs, DVDs or external hard drives
- loss of corporate ID badge
- finding sensitive / confidential information.

'Near misses' or potential risks to data security or confidentiality

Potential risks could include:

- unlocked filing cabinets
- encryption keys left in laptops
- students data left on screen
- documents left in printers, scanners or fax machines.
- Personal data left on desks

GDPR 2018 Data Breach Notification Procedure – Pinnacle Learning Trust

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 should document it. In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. 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.

Even if we feel that a breach doesn't need to be reported to the ICO, we should still document this in the College Data Breach register, along with our reasons for not doing so.

As with any security incident, we should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

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.

What information must a breach notification to the ICO contain?

When reporting a breach, the GDPR says 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
- 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

What if we don't have all the required information available yet?

We notify the ICO within 72 hours of becoming aware of the breach, explaining that we don't yet have all the relevant details, but that we expect to have the results of our investigation within a few days. Once our investigation uncovers details about the incident, we give the ICO more information about the breach without delay. However, the ICO expects controllers to prioritise the investigation, give it adequate resources, and expedite it urgently.

How do we notify a breach to the ICO?

The DPO must notify the ICO via their help line 0303 123 1113. Alternatively if we're confident that we have dealt with it appropriately, we can report it online. We may also want to report a breach online if we are still investigating and will be able to provide more information at a later date.

When do we need 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. Again, 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.

What information must we 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 The PLT DPO
- 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 our global turnover. So it's important to make sure we have a robust breach-reporting process in place to ensure we detect and can notify a breach, on time; and to provide the necessary details.

GDPR 2018 Data Breach Notification Procedure – Pinnacle Learning Trust

Procedure – Breach Notification, Data Controller to ICO

1. The employee, data subject or other persons notices a personal data breach and informs the DPO (Corinne Walker, dataprotection@pinnaclelearningtrust.org.uk),
2. Once received, the DPO will assess risk and will gather information from other relevant staff as appropriate and may assemble a team to investigate, depending on the extent of the breach. The DPO/team will assess the risk and scales of the breach by considering:
    - The number of individuals involved
    - The content of the data (is it sensitive, can individuals be identified?)
    - The likelihood of the data being returned having not been accessed/shared
    - If any measures can be put in place immediately to limit the damage
    - What is the risk to rights and freedoms of individuals concerned?
    - What is the risk to the Academy, including reputational risk?
3. The DPO will inform the Academy SLT Link (OSFC: Pamela McIlroy and Hathershaw: Mark Giles) and, if the breach is serious enough to warrant notification to the ICO or individuals concerned, the Executive Principal and Chair of Trust Board.
4. The PLT* DPO shall notify the ICO without undue delay, of a personal data breach (within 72 hours). Notification is made by phone call.
5. The PLT* DPO assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.
6. If a risk to the aforementioned is likely, The Pinnacle Learning Trust shall report any personal data breach to the ICO without undue delay, and where feasible not later than 72 hours.
7. Where data breach notification to the ICO is not made within 72 hours, it shall be accompanied by the reasons for the delay.
8. The data breach is recorded in the College Breach Register and actions taken. This will be reported to Audit and Risk Governors Committee annually.

The data controller/DPO shall provide the following information to the ICO

- A description of the nature of the breach
- The categories of personal data affected
- Approximate number of data subjects affected
- Approximate number of personal data records affected
- Name and contact details of the Data Protection Officer
- Likely consequences of the breach
- Any measures that have been or will be taken to address the breach, including mitigation
- The information relating to the data breach, which may be provided in phases.

Procedure - Breach Notification, Data Controller to Data Subject

1. Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, The Pinnacle Learning Trust DPO shall notify the affected data subject(s) without undue delay,
2. The notification to the data subject(s) shall describe in clear and plain language the nature of the breach including the information specified above.
3. Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.
4. The controller has taken subsequent measures to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.
5. Actions taken are logged in the College Data Breach register

*PLT = Pinnacle Learning Trust/Oldham Sixth Form College/The Hathershaw College