Joseph Leckie Academy

Data Breach Policy and Procedure

This policy is reviewed annually

History of Document

Approved by Governors: July 2020
Review date for Document: July 2021

Scope

This policy and procedure applies in the event that it is determined that there has been a potential breach under Article 33 (notification of a personal data breach to the supervisory authority) and/or under Article 34 (communication of a personal data breach to the data subject) of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016.

This document is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

Data controllers and data processors have different requirements and responsibilities under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016. It is therefore important to establish if the incident relates to the Academy as a controller or processor in relation to the suspected or actual breach.

This policy and procedure must be adhered to at all times without exception.

Data Protection Officer (DPO): Paul Withers
Telephone: 01922 650970
Email: InformationMgmt@walsall.gov.uk

Data Protection Lead (DPL): Cassandra Stroud
Telephone: 01922 721 071 ext. 241
Email: JLAGDPR@josephleckieacademy.co.uk

Responsibilities

All staff and contractors whether temporary or permanent are required to have an awareness of this procedure and are responsible for the reporting of any suspected or actual data breaches.

The DPL is responsible for maintaining this policy and for the reporting procedure set out in this document.

Procedure for the Academy as a Data Controller

- On finding or causing a breach, potential breach, or a security incident the staff member or data processor must immediately notify the DPL.
- The DPL will investigate the report and determine whether a breach has occurred. To decide, the DPL will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPL will alert the Principal and the chair of governors immediately.
- If deemed necessary, the DPL will contact the DPO for advice.
- The DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
    - Any safeguarding concerns

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPL will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on SharePoint.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPL expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPL will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on SharePoint.
- The DPL and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. Lessons learnt from the Data Breach will be shared with all staff.

Actions to minimise the impact of data breaches

We will take reasonable action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly high risk or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Procedure for the Academy as a Data Processor

Article 33.2 DPA 2018 places a very firm duty on data processors who must notify the data controller "without undue delay after becoming aware of a personal data breach".

The DPL will assess whether the Academy is a controller or processor when reviewing the facts and investigating a breach, suspected breach or security incident. In the event that the Academy is deemed to be a processor the DPL will inform the controller without undue delay and will assist the controller in any reasonable requests with regards to the breach or suspected breach and will make every reasonable effort to minimize the impact of the incident.