Joseph Leckie Academy

Incident Management Policy

This policy is reviewed annually

History of Document

Approved by Trustees: September 2021
Review date for Document: September 2022

1. Introduction

1.1 Joseph Leckie Academy processes personal data including special category personal data daily and it is essential that procedures are in place to ensure any threat to the security of that information is minimised and any breaches of the duties in respect of that information are identified and remedied. Any incident that compromises the security of that information, or the ICT system on which it resides, must be managed appropriately and in accordance with legislation and guidance provided by the Information Commissioners Office (ICO).

2. Purpose

2.1 The purpose of this policy is to ensure that the Academy reacts appropriately to mitigate the risks associated with actual or suspected security incidents relating to personal data. The Academy recognises that there are risks associated with users accessing and handling information to conduct official Academy business.

2.2 This policy aims to mitigate the following risks:

- Reduce the impact of personal data breach incidents by ensuring they are followed up correctly.
- Improve compliance by ensuring serious incidents are reported to the Principal and the Academy Data Protection Officer (DPO).
- To help identify areas for improvement to decrease the risk and impact of future incidents.

3. Scope

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Academy. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Under the General Data Protection Regulation (GDPR) 2016, personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2 This policy applies to all employees of the Academy, Trustees and to external organisations or individuals working on our behalf.

3.3 All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of personal data. All users have a role to play and a contribution to make to the safe and secure use of personal data and the information that it processes or stores.

3.4 You must read, understand and comply with this Policy. This policy sets out what we expect from you in order for the Academy to comply with applicable law.

3.5 Your compliance with this policy is mandatory. You must also comply with all related Policies and guidelines given. Employees who do not comply with this policy may face disciplinary action.

4. Objectives

4.1 The main objective of this policy is to ensure security incidents relating to Academy information and ICT systems are reported, recorded and investigated in accordance with the Academy's and legislative standards.

5. Legal Requirements

5.1 The Academy as data controller, must ensure that all personal data collected and held about employees, students, parents/carers, Trustees, visitors and other individuals must be protected from unlawful misuse, loss, theft, accidental disclosure, destruction, corruption or alternation in accordance with the Data Protection Act 2018 (DPA) 2018 and the General Data Protection Regulation (GDPR) 2016 as is currently set out in the Data Protection Bill.

5.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

6. Compliance

6.1 If any employee is found to have breached this policy, they may be subject to the Academy's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

6.2 Non-compliance with this policy could have a significant effect on the efficient operation of the Academy and may result in significant financial loss.

6.3 The General Data Protection Regulation (GDPR) 2016 introduces a duty for us to report personal data breaches which are significant to the Information Commissioner. This must be done within 72 hours of the breach, where feasible.

6.4 If the breach is expected to adversely impact (or has a high likelihood of impacting) individual's rights and freedoms, we must also inform those individuals 'without undue delay'.

6.5 We will keep a record of any personal data breaches, regardless of whether we are required to notify.

7. Definition

7.1 A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

7.2 This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

7.3 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.

7.4 Examples of the most common personal data breaches and information security incidents are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it. This could be verbally, in writing or electronically.
- Theft/loss of a confidential paper.

- Sending personal data to an incorrect recipient. e.g. groups of recipients such as ‘all staff' by mistake.
- Sending a text message containing personal data to all parents/carers by mistake.
- Printing or copying confidential information and not storing it correctly or confidentially.
- A non-anonymised dataset being published on the Academy website which shows the exam results of students eligible for the student premium.
- Safeguarding information being made available to an unauthorised person.
- Computer infected by a Virus or other malware.
- Finding data that has been changed by an unauthorised person.
- Use of unapproved or unlicensed software on Academy ICT equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user ID and password).
- Changes to information or data or system hardware, firmware, or software characteristics without the Academy’s knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

8. Procedure for Personal Data Breach Incident Handling

8.1 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Academy Data Protection Lead (DPL) who is the person designated as the key point of contact for Personal Data. The Academy DPL is Cassie Stroud. You should preserve all evidence relating to the potential Personal Data Breach.

8.2 On finding or causing a breach, or potential breach, The Academy DPL will must immediately notify the Principal and the Data Protection Officer (DPO) and take immediate remedial steps to mitigate and remedy the breach that has occurred. All reasonable steps must be taken to retrieve any information that has been unlawfully disclosed. The DPL will provide an initial report to the DPO. The DPO will provide advice to the Academy on any further steps that need to be taken, investigate the report, and determine whether a breach has occurred. The Principal will notify the chair of Trustees if not already notified.

8.3 The DPO will assist the DPL and relevant Academy employees or data processors where necessary to mitigate risk and impact.

8.4 The actions to be taken will be relevant to specific data types. The actions to minimise the impact of data breaches are set out below. These must, where relevant, be taken to mitigate the impact of different types of data breach. Breaches involving particularly risky or sensitive information must be acted upon swiftly and steps followed through. The effectiveness of these actions will be reviewed and amended as necessary after any data breach.

8.5 **Example:** If sensitive information has been disclosed via email (including safeguarding records) or other special category data (sensitive information) such as health information is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Where this is unsuccessful or not possible immediate steps should be taken to contact the recipient with instructions to them to delete the email.

If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the ICT department to recall it.

8.6 Where Academy employees receive personal data sent in error they must alert the sender and DPL as soon as they become aware of the error.

8.7 In any case where the recall is unsuccessful, the DPL will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. The DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

8.8 The DPL will notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies.

9. Investigation and Report

9.1 The DPO will carry out an internet search to check that the information has not been made public. If it has, the DPO will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

9.2 The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

9.3 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

9.4 If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the personal data breach coming to the attention of the DPL.

9.5 The DPO 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.

9.6 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

9.7 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 DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

9.8 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 advise the DPL to 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

10. Report

10.1 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 securely on SharePoint.

11. Review and Planning

Upon the occurrence of a serious breach the DPO and DPL will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible. A report of the data protection breache will be presented to the Principal and the Trust Board.

12. Further Information and Associated Policies

12.1 For further information about Information Governance please visit the ICO website www.ico.org.uk

12.2 This policy should be read alongside:

- Information Governance Strategy
- Information Risk and Security Policy
- CCTV Policy
- Data Protection Policy
- Confidentiality Policy
- Freedom of Information Policy
- Information Rights Policy
- Records Management Policy and Schedule
- Subject Access Request Policy
- Consent to Use Personal Data Guidance

- Impact Levels and Protective Marking Guidance