Data Breach Plan and Procedure

Dec 2024

CIFA Data Breach Plan and Procedure

Doc Number: DBPP

Version 2 03/2025

Following Review 03/2026

1. Purpose

This Data Breach Plan and Procedure outlines the steps CIFA Education Ltd will take in the event of a data breach. It ensures compliance with the UK GDPR and aligns with our existing policies, **please refer to the GDPR Compliance and Data Handling Policy (Doc Ref: GDPR)** to protect the rights and privacy of individuals whose data we process.

2. Scope

This plan applies to all personal data held by CIFA Education Ltd, including electronic and paper records. It covers data breaches resulting from unauthorised access, accidental disclosure, loss or destruction of personal data.

3. Roles and Responsibilities

- **Compliance Officer**: Oversees data protection compliance and manages breach response.
- **All Staff and Contractors**: Must report suspected data breaches immediately and cooperate with the investigation.

4. Identifying a Data Breach

A data breach may involve:

- Unauthorised access to personal data
- Accidental or unlawful destruction, loss or alteration of data
- Unintended disclosure of personal information
- Cyber security incidents leading to data compromise

5. Reporting a Data Breach

- Any individual who suspects a data breach must report it immediately to the Compliance Officer via email or other established communication channels.
- The report should include:
    - Date and time of the breach discovery
    - Nature and extent of the breach
    - The type of personal data affected
    - Potential risk to individuals

6. Containing and Assessing the Breach The Compliance Officer will:

- Investigate the breach and confirm its extent
- Take immediate action to contain and mitigate further exposure (restricting access, recovering lost data and notifying IT security professionals if applicable)
- Assess the risk to individuals and the organisation
- Determine whether external parties (IT support, legal counsel) should be involved. Refer to our **IT Security & Acceptable Use Policy, (Doc Ref: ITSAP).**

7. Notifying Affected Individuals and Authorities

- If the breach poses a high risk to an individual's rights and freedoms, affected individuals must be notified without delay.
- If required by law, the Information Commissioner's Office (ICO) must be notified within 72 hours of becoming aware of the breach.
- Notification should include:
    - The nature of the breach
    - The potential impact on individuals
    - Measures taken to address the breach
    - Advice for affected individuals to mitigate risks

8. Documentation and Review

- All breaches must be documented in the Data Breach Register, including details of the incident, response actions and lessons learned.
- The Compliance Officer will review each breach and recommend changes to prevent recurrence.
- The Data Breach Plan and Procedure will be reviewed annually and updated as necessary.

9. Preventive Measures

- Regular staff training on data protection and breach response
- Implementation of strong access controls and encryption
- Regular security assessments to identify vulnerabilities

10. Contact Information:

For any data protection concerns, please contact: the Compliance Officer, our current acting officer is eze@cifa.ac