Data Breach Policy

Author: Paul Vincent
Date: 23/02/18
Status: Published

1. Introduction

The Open College of the Arts as a distance learning educational institution is required by its function and relevant regulatory bodies to obtain and hold personal, financial and education history data on its students. In addition, the college also holds relevant personal and financial data on its staff and tutors. Although every effort is made to ensure this data is held and transmitted in a secure state, the event of a data breach (a loss of control or possession over the data held) and its ramifications for the individual, and the college must be considered, alongside the need for auditable mitigating processes.

2. Purpose of this policy

The Open College of the Arts is required under the present Data Protection Act 1998, and the forthcoming General Data Protection Regulation (GDPR), to ensure it has sufficient processes in place to ensure the security and confidentiality of its stakeholders' personal and financial data. In the event of a failure of these processes, the college is required to have in place clear and robust methods and policies in place to deal with a data breach event.

The policy aims to minimise the negative effects of any data breach event and contain the extent of the breach through application of the guidance and processes it contains. It also aims to provide a process by which the risk of future similar breaches can be reduced.

This policy sets out a series of protocols for the reporting, containment, mitigation of, and recovery from, data breach events for employees to follow in the event of such a data breach occurring.

3. Definition of a Breach

A Data Breach is an event that results in the loss, corruption or theft of data held by a data controller (in this case, the Open College of the Arts) or Data Processor (this might be one of the college's service providers, e.g. Google, or Openathens.) The breach might involve just basic personal data, such as an individual's email address or name, or might involve sensitive data, such as financial or medical records. In all such cases, the breach must be reported upon and dealt with in accordance with this policy and its protocols.

4. Results of a breach

A breach may result in: compromise of sensitive information, loss of confidentiality, integrity, or availability may result in physical or financial harm to individual(s), reputational damage, a detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Failure to report a breach to the appropriate authorities can result in the application of a 10,000,000 Euro fine due to non-compliance with GDPR.

5. Scope

This document deals with the mitigation and reporting of data security breaches relating to all forms of personal and financial data, regardless of the format or context in which it is held.

This policy applies to all college stakeholders; staff (including contracted personnel, tutors and trustees of the college), service providers to the college, students and active alumni (e.g. College Alumni performing designated duties as, for example, advocates.)

6. Data Breach Categories

Most data breaches will fall into one or several of the following categories of data breach:

- Physical loss of equipment containing, or suspected to contain, personal or financial data. E.g. data storage devices, laptops, desktop computers, paper documents.
- Infiltration of college systems and the subsequent extraction of confidential data (even if held in an encrypted state) from those systems.
- Unauthorised disclosure (verbal, or textual via paper or electronic transfer) of sensitive information.
- Web-service infiltration and assumed data extraction.
- Email or telephone scams resulting in the sharing of personal data.
- Extraction of data (encrypted or otherwise) in transfer via unsecured wireless networks.
- Access to sensitive data by unauthorised individuals.

7. Reporting a Data Breach Protocol

If any stakeholder of the college suspects a data breach has occurred, they must immediately report the incident via the **Data Breach Report Form**, or if that form is not available or cannot be accessed, to both the college's IT help desk: help@oca.ac.uk and to the Head of Technology and Media: paulvincent@oca.ac.uk for the matter to be investigated and dealt with as a matter of urgency.

7.1 Report content

A report of a data breach must contain the following information at minimum:

- Name of individual reporting the breach
- Contact details of the individual reporting the breach
- Nature of the breach - what system it affects, and which individuals if applicable

- Date and time of the breach
- Crime Reference Number (if applicable)

Please refer to the Report form at the end of this paper for full details of the required information.

If a breach occurs outside of working hours, the report will be picked up and dealt with as early as possible.

If the breach involves the loss or theft of equipment, this must be immediately reported to the police and a Crime Reference Number obtained.

7.2 Failure to Report

A failure to report a known data breach by any member of college staff could result in **the college being fined up to a maximum of 10 million Euros, and *will* result in the college's Disciplinary Procedures being put into effect.**

Following a review of the breach incident, any employee, contractor or student found to have been the cause of the breach will be subjected to the college's disciplinary procedures.

8. Process of Containment, Mitigation and Recovery of Service

8.1 Containment

Following receipt of a data breach report, the first step must be to establish whether the breach, and its causes are ongoing or already contained. If the former, the Technology and Media team will prioritise the containment of the data breach above all other responsibilities until the breach is contained.

8.2 Analysis

Following containment, an analysis and report on the scale and severity of the breach will be conducted by the Head of Technology and Media, prior to handing over the process to the most relevant member of staff (the designated Lead Investigating Officer - LIO), depending upon the specifics of the breach.

8.3 Mitigation / Recovery

The LIO will determine whether any lost data can be recovered and to what extent the damage (to individuals, systems, and the organisation itself) can be mitigated. Any identified actions to achieve these ends will be set in motion at this point.

8.4 Report

Depending upon the scale and severity of the breach (see next section) the LIO will then inform the relevant authorities; e.g. the ICO (https://ico.org.uk/for-organisations/report-a-breach/)

and/or the police if an incident is deemed severe enough to warrant it; e.g. the loss of individuals' bank details, or other highly sensitive data which might be used with criminal intent.

The LIO will, through collaboration with other relevant members of the organisation, determine the most suitable course of action for addressing the breach and its causes.

9. Investigation and Risk Assessment

An investigation will be undertaken by the LIO within one working day of the data breach occurring or having been discovered or suspected to have occurred.

Risks associated with the breach will be considered by the LIO, in consultation with relevant Heads of departments and Directors wherever appropriate. The severity of each associated risk will be determined, alongside the likelihood of such an incident recurring.

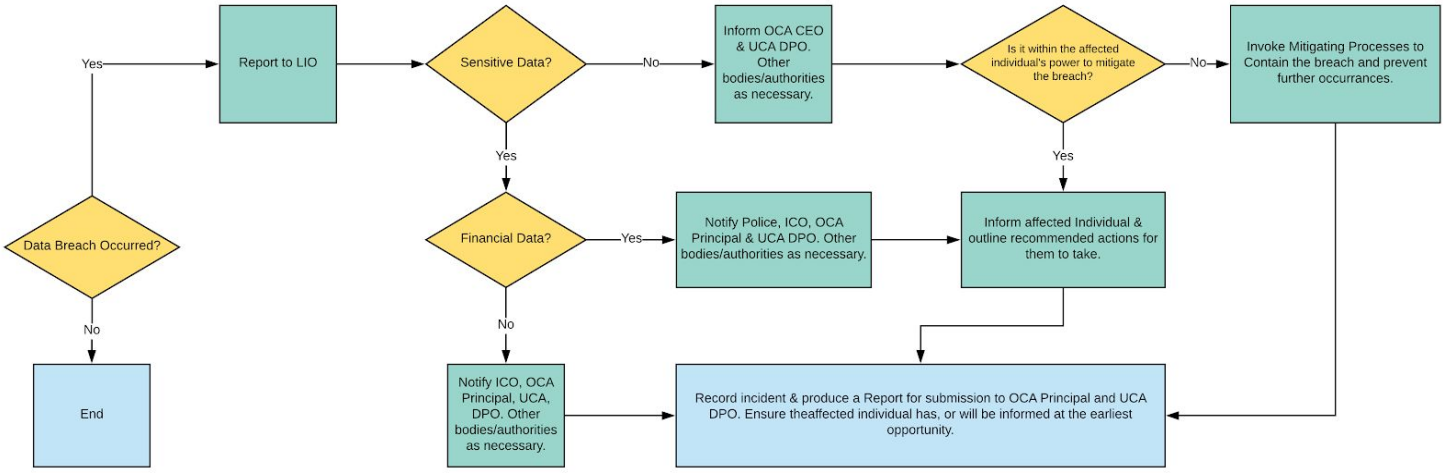
The investigation will take into account the following:

- the type of data involved
- its sensitivity
- the protections in place, or lack thereof (e.g. encryption, 2FA)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

10. Required notifications

The LIO and other relevant and informed members of staff will determine through an examination of the scope, scale and severity of the breach, which parties, if any, are required to be informed.

The following process should be followed in the event of a data breach event occurring.



Considerations will include:

- Any regulatory and/or legal requirements to notify specific individuals affected or relevant bodies or authorities.
- An assessment of whether disclosure of the breach will either assist the affected individual in reducing the effect of the data breach, or assist in preventing the unlawful and potentially damaging use of the data.
- If the scope, scale and severity of the breach warrant it, the ICO must be informed of the data breach within 48 hours of it first being reported.
- Whether notifying all affected individual will, in consideration also of the scope, scale and severity of the risk, unduly cause alarm and an increased workload for frontline staff.

If the breach is sufficiently serious, relevant authorities, e.g. ICO, police, insurers, UCA, trade unions, will be informed of the full details of the breach, and the steps being taken to reduce its impact and prevent future occurrences.

10.1 Notification content

Affected individuals will be notified of the:

- Nature of the breach, including data believed to have been lost or acquired.
- Date and time of the breach.
- Ways in which they themself can mitigate against the impact of the breach.
- Steps being taken to recover the data and prevent further breaches.

A PR campaign may be required to counter any adverse publicity in the media. Relevant details which do not divulge details of any security processes or systems to be provided for incorporation into such a campaign.

11. Review

Following containment and the establishment of any immediately required preventative measures, a full review is to be conducted by the Head of Technology and Media into the context, nature, and fallout from the Breach Event. The review must include:

- In what location(s) and in what state the personal data was held
- Any significant risks must be identified and what Risk Response was taken or should have been taken during this incident
- Establish that any transmitted data was secured, and if not, why not
- Establish in what ways (if at all) the scope of the breach was mitigated by the imposition of robust permissions structures.
- Recommendations for improvements to Data Protection systems, workflows, and policies.

The review will in the first instance be submitted to the college Principal, who will then make a judgement on whether the issue should be referred to the Board of Trustees.

The Data Breach Reports sheet must be updated following the Review process.

12. Document Control

Document Name	Data Breach Policy
Document Number/Version	POL-DP-001/1
Document Author	Paul Vincent | Head of Technology and Media
Approving Body	OCA Executive Group
Signature of Approval	
Date of Approval	08/05/18
Date Effective from	08/05/18
Review Date	01/10/18
Document this supersedes	N/A
Is this document for public access	Yes