Data Breach Policy
August 2024

1. Policy Summary

1.1. 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 employees. 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.

1.2. The Open College of the Arts is required under the Data Protection Act 2018 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.

1.3. 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.

1.4. 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.

1.5. 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.

1.6. **Failure to report a breach to the appropriate authorities can result in the application of a 20,000,000 Euro or 4% of global turnover fine (whichever is greater) due to non-compliance with the UK's Data Protection Act 2018 and the EU GDPR 2018.**

2. Scope

2.1. What does this policy cover?

2.1.1. This document deals with the mitigation and reporting of data security breaches relating to all forms of personal and special category data, regardless of the format (physical, audible or digital), or context in which it has occurred.

2.1.2. This policy applies to all college stakeholders; employees (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.)

3. General Principles

3.1. The OCA has a duty of safeguarding over its students and employees. The protection of personal data is a key aspect of that duty of care.

3.2. As a controller of data obtained and processed by consent, the college has a duty of care over the consensual data it controls and processes.

4. Protocol for reporting a Data Breach

4.1. 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 the college's dedicated email: DPO@oca.ac.uk for the matter to be investigated and dealt with as a matter of urgency.

4.2. 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 - which systems and/or individuals are affected?
- Date and time of the breach
- Crime Reference Number (if applicable)

4.3. If a breach occurs outside of working hours, the report will be reviewed the next working day and if it meets the threshold for reporting to ICO, the report must be issued no later than within 72 hours of the breach being reported.

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

5. Failure to Report

5.1. A failure to report a known data breach by any employee could result in the college being fined up to a maximum of 20 million Euros, and will result in the college's Disciplinary Procedures being put into effect.

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

5.3. Where human error is the cause, the individual's line manager should be informed of the circumstances; they will then, in light of the DPO's advice and the LIO's report, consider whether the college's disciplinary procedures need to be invoked.

5.4. Where the individual at fault is a student, the incident should be reported to the Student Services team who will consider whether the college's Student Code of Conduct policy has been breached.

6. Process of Containment, Mitigation and Recovery of Service

6.1. 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.

6.2. Analysis: Following containment, an analysis and report on the scale and severity of the breach will be conducted by the DPO, prior to handing over the process (if necessary) to the most relevant employee as the LIO, depending upon the specifics of the breach.

6.3. 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.

6.4. Report: Depending upon the scale and severity of the breach (see next section) the LIO will then inform the DPO who will 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 special category data which might be used with criminal intent. The DPO and 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.

7. Investigation and Risk Assessment

7.1. 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.

7.2. 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, policies)
- 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

8. Required communications

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

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 72 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 employees.
- Whether the fault lies with a system or with an individual. In the latter case, the LIO should inform the individual at fault's line manager, who may then wish to consult further with the LIO and DPO prior to making any decisions regarding disciplinary or remedial actions.

8.2. If the breach is sufficiently serious, relevant authorities, e.g. ICO, police, insurers, The OU, 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.

8.3. Communications content

8.3.1. 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.

8.3.2. 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.

9. Review

9.1. Following containment and the establishment of any immediately required preventative measures, a full review is to be conducted by the Data Protection Officer 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
- Whether the breach was caused by system failure or human error
- 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, policies and training.

9.2. 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.

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

10. Compliance Measurement

10.1. The college will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the DPO (dpo@oca.ac.uk), policy owner and Senior Management Team (smt@oca.ac.uk).

10.2. Exceptions

10.2.1. There are no exceptions to the policy; all suspected data breaches must be reported according to the policy.

10.3. Non-Compliance

10.3.1. Any employee found to have violated this policy may face repercussions, up to and including termination of employment.

11. Glossary of terms

11.1. **Data Controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. This will in the majority of cases be the Open College of the Arts, but there may be situations where the college acts as the processor of data controlled by another person or entity.

11.2. **Data Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

11.3. **Personal data:** information about who you are, where you live, what you do and more. It's any and all information that identifies you as a data subject.

11.4. **Special category data:** types of data that require additional protections due to their sensitive nature. For example, medical, genetic or biometric data; race or ethnic origin; religion; trade union membership status; sexual orientation; criminal history or political beliefs.

11.5. **Data Protection Officer (DPO):** the individual responsible for managing reports of data breach events, and for providing advice on the reporting process.

11.6. **Data subject:** someone who can be identified from personal data.

11.7. **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 (e.g. a service provider such as Google, Meta, JISC etc.) The breach might involve personal data, such as an individual's email address or name, or might involve 'special category' data. In all cases, the breach must be reported upon and dealt with in accordance with this policy and its protocols.

11.8. **Lead Investigating Officer (LIO):** the individual tasked with investigating details of the data breach following the reporting of a breach having occurred. If the DPO does not assign themselves to this role, the DPO will assign the LIO role to an appropriate employee.

12. If you need support

12.1. For support in adhering to this policy, please refer to the college's Data Protection Officer (dpo@oca.ac.uk) or your own line manager, or other management employee, for advice.

13. Linked and other policies and legislation

13.1. UK Data Protection Act 2018

13.2. EU GDPR 2018

13.3. Data Protection Policy

13.4. Information Security Policy set

13.5. Email and Communications Policy

13.6. Network Security Policy

13.7. Student Code of Conduct policy

13.8. Data Breach Report Form

14. Changes since previous policy

14.1. The Policy has been reformatted to use the college's new Policy Template.

15. Policies superseded by this document

15.1. This Policy replaces version 1 of the Data Breach Policy.