Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

OCA Data Breach Procedure

Updated: June 2023

Purpose

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.

The Open College of the Arts is required under the present 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.

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.

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 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.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

Values / principles

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

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.

Scope

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.

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.)

Changes

- Since the last version of the policy, the following changes have been made:
- Document changed from Policy to Procedure
- Section added on what is personal data
- Section added on the ICOs key points
- Details on how to call/email added in the procedure
- Update made on how to contact the Information Rights Team
- Updates made on when the OU DPO needs to be contacted
- Step 8 to 9 added on investigating a personal data breach
- Information added on the ICO notes about risk
- Updates made to the required communication for data breaches
- Details added if an individual is already aware of a breach
- Information added if a partner needs informing
- Details of Infosec added in the policy
- Risk assessment details added
- Section added on additional aspects to consider when working on personal data breaches
- Removed Appendix C: Data Breach Response Diagram

Related policies and legislation

- UK Data Protection Act 2018

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

- EU GDPR 2018
- Data Protection and Confidentiality Policy
- Workspace Security Policy
- Email and Communications Policy
- Network Security Policy
- Student Code of Conduct policy
- Data Breach Report Form

Policy / procedure

1. What is a Personal Data Breach

The Information Commissioner's Office defines a Personal Data Breach as follows:

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

The Information Commissioner's Office further breaks this definition down by using the Information Security triad of Confidentiality, Integrity and Availability

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 accidentally lost, destroyed, corrupted or disclosed; (Confidentiality)
- if someone accesses the data or passes it on without proper authorisation; (Integrity)
- or if the data is made unavailable and this unavailability has a significant negative effect on individuals (Availability)

Some common Personal Data Breach examples include:

- Disclosing personal data (e.g., in an email) to an incorrect recipient
- Access of personal data by an unauthorised third party
- Computing devices containing personal data being lost or stolen

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

- Incorrect access controls (e.g., giving access to a SharePoint site containing personal data to someone who doesn't need it)
- Leaving papers containing personal information on a train

Information Commissioner's Office (ICO) Guidance and Key Points

- The Information Commissioner's Office is the '*UK's independent body set up to uphold information rights*.'
- As a Data Controller, The Open College of Arts is obligated by law to report 'notifiable' breaches to the ICO
- 'Notifiable' breaches are those which are likely to result in a risk to the rights and freedoms of individuals

- Article 33 of the GDPR notes the following:
  - *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.*
  - 'Notifiable' breaches must therefore be reported to the ICO within 72 hours from the point that any colleague/individual becomes aware of/suspects that there has been a personal data breach

- Detailed ICO guidance on data breach reporting can be found here - UK GDPR ICO Data Breach Guidance.

2. Protocol for reporting a Data Breach

2.1. 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.

2.2. 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)

2.3. 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.

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

Call/Email

- Call/Email reports are also received for Personal Data Breach notifications. Calls can be made to the college on 01226 978330
- These are infrequent and will require either:
  - The DPO requesting the colleague/contact to fill out the Personal Data Breach form
  - Or alternatively, the DPO fill out the Personal Data Breach form based on the information provided via the call/email

3. Failure to Report

3.1. 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 20 million Euros and will result in the college's Disciplinary Procedures being put into effect.

3.2. 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.

3.3. 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 Lead Investigating Officer (LIO) report, consider whether the college's disciplinary procedures need to be invoked.

3.4. 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.

4. Process of Containment, Mitigation and Recovery of Service

4.1. The Open College of Arts shall liaise with The Open Universities Information Rights Team (IRT) when necessary to assist with the process of containment,

mitigation and recovery of service of data breaches. OCA can contact the IRT by emailing oca-info-rights@open.ac.uk.

4.2. 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. One of the first steps will also be to establish whether personal data is actually involved. 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 the team shall liaison with the OU's Information Rights Team

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

4.4. Mitigation / Recovery: The LIO with assistance from the OU's Information Rights Team 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 Report: Depending upon the scale and severity of the breach (see next section) the LIO will then inform the DPO. OCA DPO and OU DPO shall discuss the breach and 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 OU DPO, OCA 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.

5. Investigation and Risk Assessment

5.1. 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.

5.2. Risks (risk to the data subject or OCA) associated with the breach will be considered by the LIO, in consultation with the DPO and 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:

Step 1 – When was the potential personal data breach discovered?

- At what point was it discovered that there was a potential personal data breach?
- The law details that any reportable data breaches must be reported to the regulator (ICO) without undue delay and within 72 hours of a personal data breach being identified.
- This is a key part of the risk assessment as it will show how much time is available to ascertain facts, risk assess the breach and then provide information to the ICO in time.

Step 2 – Check if personal data is actually involved

- Has personal data actually been breached by being disclosed, altered, destroyed etc.
- Or is the data e.g., business information which is not classed as personal data and therefore the case would not be handled as a personal data breach?
- It is advisable to view a copy of any associated documents when e.g. an email has been sent to a student/colleague in error. This will assist in determining exactly what personal data is involved and potential inferences.

Step 3 – Establish what personal data has been breached?

- What types of personal data have been breached? (e.g., email address, name, date of birth, address etc.)
- Is there a special category/sensitive data angle? (Trade Union Membership/Disability Support/Occupational Health etc.?)
- Is there a financial information angle or sets of personal data that could lead to increased risk of identity fraud?
- If it's not fully defined what personal data has been breached and how much – you will need to consider how to get this and who to liaise with. This information is crucial in order to fully understand, and risk assess a personal data breach

*Depending on the circumstances of the breach, who has the information on an unauthorised basis etc. these scenarios need to be dealt with and risk assessed carefully as the potential impacts on data subjects could be high

and harmful (e.g. sensitive personal data of vulnerable people/financial information leading to identity fraud)

Step 4 – Consider who might have the personal data

- Who specifically has received personal data incorrectly/has access to it etc.
  - **Internal colleagues**
    - If an internal colleague has access/been sent data incorrectly – it's likely that containment can be actioned swiftly and mitigated against. Given that colleagues work under OCU codes of conduct/have completed GDPR training and know what expectations are
    - However, if a colleague receives information that is in relation to a co-worker, then the risk assessment may be different dependent on the severity of the personal data breach and the types of personal data that has been exchanged/accessed.
  - **Students**
    - If a student has been sent a document in error – what type of document has been sent? What information is included?
    - Is there information about fellow students on the same module? Which means there is a high risk that the data subject who had their data sent on may find out?
  - **External contact**
    - Is this a partner organisation?
    - Member of the public who has received something in error?
  - **Malicious actor?**
    - What has been done to contain the breach. I.e. if login details have been gained have login details been changed.
    - What are the potential consequences?
    - Is there potential for identity fraud
    - Potential for personal data being passed on to further malicious actors?
    - Harm to the data subjects' rights and freedoms – e.g. are they being sent unwanted communications? Could be at higher risk of spear phishing? Changes to e.g., bank accounts without their authorisation etc.?
  - **Personal data left in a public place**
    - Is the location of the data known?

- If it is left at a venue with known OU contacts – have they been contacted?
- They can secure the documents and mitigate any future risk
- Is the data in a secured building?
- Documents can be located and secured. Mitigate against any breach
- Has it been left on public transport?
- Service providers contacted
- If a PC – can the contents be wiped remotely
- Did the PC have a password/encryption on it to safeguard any data
- Has a login been left live on a public computer?
- Possible to force a log out via Information Security
- Can track other users of the PC? Or determine how many other users there may have been

Step 5 – Work out how many people might be affected?

- Who has had their data breached
- How many data subjects
- Who has had access to the information incorrectly
- Who is involved in the personal data breach case – which units, which teams, which third parties (contractors/third party processors etc.) specifically, who are the owners of access controls etc., creators of policy, oversight of an area etc.

Step 6 – Consider how seriously it will affect people

- Are the people involved vulnerable adults or children?
- Is it likely the breach will put someone in an unsafe situation?
- Are people at risk of losing money, their job or their home as a result of the breach?
- Do you know how the breach will impact people's health and wellbeing?

The above will assist with assessing risk of harm and impact on rights and freedoms also.

Step 7 – Containment

- Has the case been contained at all? Are containment actions required immediately? Before containment is carried out is further information required?

Tips/guidelines for containment measures (top 4 bullets taken from ICO guidance)

- If something is sent to someone by mistake, you can ask them to delete it and provide confirmation that they won't share anything seen/downloaded etc. further
  - Doing this ensures that any further sharing of information is unauthorised and would constitute a 'breach of confidence'
- Amend access controls – e.g., if a SharePoint site/document has the wrong permissions
- If a template has been amended with Personal Data in error – arrange for this to be made private, amended and review how this is stored and access going forwards
- If something has been stolen, like a laptop and systems are installed which enable to be wiped can action this immediately. Will minimise the risk of the personal data falling into the wrong hands
- Can contain a cyber incident by changing all passwords and making affected colleagues do the same
- System updates
- Collaboration with stakeholders

Step 8 – Document everything else you know about the breach

- What other factors are there in the personal data breach scenario
- Are there any other system related issues, wider access controls issues that need to be documented
- Are there any training and awareness pieces that have been identified through the case?
- Does the personal data breach link to any other known issues or personal data breaches
- Is there an emerging pattern?
- Note down the steps taken so far – if there are related instances which emerge – find out more details about these

Step 9 – Assess the risk

The ICO notes the following about risk:

> *Risk in personal data breaches means the risk to the people whose data may have been breached.*
>
> *A risk assessment, in personal data breach terms, is where you think about how seriously you think people might be harmed and the probability of this happening.*
>
> *Your risk assessment should take into account who might be affected, how many people might be affected and the ways it might affect them. There will always be other risks for you to consider, such as the risk to your reputation, or financial loss, but your first response should be to*

look at the risk to individuals and think about any steps you can take to reduce that risk or help them in some other way.

Whether or not it's a high-risk situation depends on what the personal data is and what could potentially happen with that data. If you decide it's unlikely there will be a negative impact on those concerned, you might categorise it as low risk. However, if the potential consequences are very significant, you might consider the overall risk assessment to be high, even if it's unlikely to happen.

In every situation, levels of risk can vary, and your decisions might change as new information becomes available.

When a personal data breach is reported in, it's important to carry out a risk assessment. This is on the basis of the following:

- Need to understand what data is involved in the data breach?
  - Is it personal data or not?
  - Is there special category data involved?
- How many people have been affected?
- What harm has, or potentially will affected data subjects as a result of the personal data breach?
- Is the personal data breach reportable to the ICO? If it is, it needs to be reported to the ICO within 72 hours without undue delay

In addition to all of the above, a record of the personal data breach, data subjects involved, and the College's decision-making process should be documented to enable:

- The ICO/College Management to carry out a full audit of previous breaches should this be required
- Allow for effective OCA DPO and OU DPO or ICO review of any case – should a complaint be raised

Key things to take into account when trying to risk assess a personal data breach (information taken from ICO website on Understanding and assessing risk in personal data breaches | ICO)

6. Required communications

6.1. The OCA DPO and OU DPO 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.

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 staff.
- 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.

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.

Please note: GDPR legislation does not stipulate that data subjects are advised pro-actively when a case is determined as being non notifiable. Pro-actively advising a data subject in this case would be at the Controller's discretion and should be carefully considered

Already aware

- Data subjects may be aware if they are reporting in a personal data breach, have had notification of their personal data being affected etc.
- In some cases, colleagues may pro-actively advise affected data subjects ahead of reporting to the DPO if they have sent an email to the incorrect recipient etc.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

6.2. Does a Partner need informing?
The College has many partnerships with third parties (e.g. Employers, System providers) and therefore where there are cases which straddle both OCA and third party services – consideration should be made whether a Partner should be informed. (This should also take into account any provisions noted within relevant data sharing or data processing agreements)

6.3. Communications 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. Advise and assistance must be sought from OU DPO before any information is issued in the media.

6.4 Information Security (Infosec) Reference
Personal Data Breach cases can have Information Security angles to them When cases are being worked on by both Information Security and the DPO team – the Information Security reference number should also be noted.

7. Review

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.

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.

8. Additional aspects to consider when working on Personal Data Breaches

A. Personal Data Breach Culture

- The Open College of the Arts are focussed on operating a 'no blame' personal data breach reporting procedure. The rationale for this is as follows:
  - Encourages Personal Data Breaches to be reported in
  - Build rapports with stakeholders and ensures effective engagement when working through containment steps and solutions
  - Builds a positive network and ensures that colleagues do not feel inhibited or apprehensive in reporting Personal Data Breaches when they occur

- On the basis of the above, when Personal Data Breaches are reported in, the primary focus is on
  - Understanding the full details of the Personal Data Breach
  - Containment
  - Future mitigation
  - Raising awareness with colleagues who may have made the error and providing support with this where appropriate.

- There are certain cases where the DPO may flag directly with a colleague's Line Manager that they need some pro-active support, assistance and discussion to be had (as there may be some mitigating circumstances that only the Line Manager would know/colleague to disclose)

  - If there have been more than e.g., three personal data breaches reported
  - If a Personal Data Breach occurred which was medium/high in risk rating to
    - Raise awareness
    - Discuss the risks about any other similar Personal Data Breaches occurring
    - Ensure that the colleague has a support mechanism in place

- Ensure future risks are mitigated against positively

B. Key points of contact to engage when working on a Personal Data Breach case

- Colleague who reported in the Personal Data Breach
  - If this is the Line Manager of the colleague who made the error or the colleague themselves – liaise with them directly by phone/email to Understand the full and further details

  Build rapport and discuss future mitigation mechanisms

- **Information Security**
  - Where a Personal Data Breach has an Information Security angle e.g. associated with systems and their set up (e.g. Google Drive permissions; Student Information System permissions etc.) or to do with identity fraud (e.g. a malicious actor has contacted Student Support acting as the student or a student's login has been hacked) it's important to engage Information Security
  - Information Security and the Data Protection team work collectively on such cases to ensure all bases are covered

- **OCA DPO/OU DPO**
  - Where cases appear to be high risk – these should be flagged with the DPO for assessment
  - Any cases which go to the ICO are referred to the OCA DPO and OU DPO for assessment and input prior to a decision being finalised about notification
  - Cases which link to the following should be flagged at the earliest opportunity
    - High risk to rights and freedoms (likelihood and/or severity)
    - Special Category Data (where there is a high risk)
    - For large quantities of personal data of either category

C. Line Manager

- The Line Manager of the colleague who made the error is approached in these ways:
  - The colleague who made the error is usually advised to inform their Line Manager autonomously. This builds a culture of trust and gives the colleague to engage with their Line Manager directly and take ownership of this
  - Where a colleague's error has been determined but neither the colleague or Line Manager is aware – it's best practice to contact the Line Manager to raise awareness with them tactfully so that they can sensitively raise this with their direct report and be based placed to immediately support them

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

D. How to determine if a case is a low-level case

- The recipient of information does not represent a risk
  - E.g., if a colleague received an email in error
  - E.g., if a colleague was able to view information in error
- The level of personal information disclosed is minimal
  - E.g., if a student's PI only was disclosed in an email to another student in error
- The recipient has flagged the case and has pro-actively asked whether to delete or has already done so
  - E.g., if a student received an academic reference for another student. Address, PI details would be on this. However, if the student has flagged this, they are likely to follow containment actions of deleting the document/not sharing further

E. How to deal with/determine if a case is a higher risk case

- The case involves special category data
  - E.g. disability information, grievance, dismissal
- Data has been disclosed which puts the data subject in potential position of harm/infringements to their rights and freedoms
- Disclosed to a recipient which means:
  a) the recipient is likely to use maliciously or harm,
  b) knowledge of the information is harmful
  c) recipient is a malicious actor and control or transmission of data is not possible

F. Guidelines on how to report cases to the ICO

- ICO form and guidance is here: ICO - Report a Breach

G. Post case lessons learned to stakeholders

When discussing personal data breach cases with, Line Managers and colleagues - some of the common post-case advice includes:

- Mis-Emails
  - Use of BCC function
  - Careful use of Gmail autofill
  - Encrypt documents
  - Check twice and send once
- Data Minimisation
  - Seek to review what information is being held or transferred
  - Is the data set scope still relevant and required
  - If there is surplus information being transferred or recorded etc. this should be amended

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

- Data Accuracy
    - If information is being recorded via an incorrect process method, or on the wrong student/colleague record – review this and seek to update to ensure accuracy
    - If data is being transferred from one team to another – what protocols and safeguards are in place to ensure data is transferred a) securely and that b) the data integrity is maintained
- Document Transfers
    - For OU transfers, do this via ZendTo
    - Encrypt with passwords
    - Place documents on a shared and access controlled space (MS Teams/SharePoint) and send a link to this rather than send documents on. Mitigate against incorrect recipients receiving the data and quick access to point to amend data/delete should this be required.
- Access Controls
    - Review of how these are structured in e.g. Google Drive or MS SharePoint
    - Processes in place to ensure when there is staff turnover that these are reviewed and amended accurately
    - Recommend that permissions are reviewed on a regular basis
    - That owners are clearly defined and know their responsibilities
- Training and Awareness
    - Reminders to colleagues/teams
    - Re-visit GDPR training
- Process reviews
    - Teams to review their processes on various Data Protection elements
        - To enhance compliance by design and default
        - Prevent breaches
        - Assist with colleague understanding
- System changes
        - System structures require fundamental changes?
        - Automation to assist with adherence to principles
        - Automation to assist with mitigating human error

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

Implementing the policy

Compliance Measurement

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).

Exceptions

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

Non-Compliance

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

Support for the policy

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 staff, for advice.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

Appendix A: Definitions

- **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.
- **Data Processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- **Personal data (PII)**: 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.
- **Special category data (SPII)**: 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.
- **Data Protection Officer (DPO)**: the individual responsible for managing reports of data breach events, and for providing advice on the reporting process.
- **Data subject**: someone who can be identified from personal data.
- **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.
- **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 member of staff.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24

Appendix B: Forms of Data Breach

The following is a (non-exhaustive) list of the types of data breach you are most likely to encounter:

- 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 e.g. relating to financial or medical details, race, religion, sexual orientation or other personal/private information, and any other sensitive information that shouldn't be disclosed to anyone outside of the institution.
- 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 individual

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Published	Paul Vincent	OCA Principal	August 2023	01/08/24