Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

OCA Data Protection and Confidentiality Policy

Updated: July 2022

Purpose

OCA takes very seriously its responsibility to manage data securely and to respect individuals' confidentiality to ensure its compliance with the General Data Protection Regulation (GDPR).

The purpose of this policy is to ensure individuals' rights to privacy and protections under the UK Data Protection Act 2018 and the EU GDPR are maintained both during and following an individual's associations with the college.

The primary objectives of the Policy are that information must be:

- Fairly and lawfully processed
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than is necessary
- Processed in line with individuals' rights
- Secure
- Not transferred outside the European Economic Area without adequate protection.

Values / principles

There are seven principles of data protection as set out in the GDPR 2018 EU Regulation, which inform this and related policies:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Scope

This policy applies to all OCA students and employees in addition to any third parties who may be required to provide services and/or consultancy work for the college.

All students and employees at OCA have a responsibility to ensure that the rights, under the UK Data Protection Act 2018, of any individual they may interact with through their roles as students or employees of the college, are maintained in accordance with the requirements and expectations laid out in this policy.

All employees are required to undertake mandatory Data Protection training during each year of their employment at the college.

Changes

Since the last version of the policy, the following changes have been made:

Updated to use the college's revised Policy Template

Incorporated sections on: Right to restriction; Right to rectification; Right to portability; Right to object and 'Implementing the Policy.

Replaced references to Privacy Shield with Standard Contractual Clauses.

Policies superseded by this document

Data Protection and Confidentiality Policy, version 1, 27/11/18

Related policies and legislation

This policy references:

- UK Data Protection Act 2018

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

- EU GDPR 2018
- Student Computing Policy
- Email and Communications Policy
- Data Protection Impact Assessment (DPIA) Policy
- Network Security Policy
- Data Retention Schedule
- Data Breach Policy
- Data Breach Report Form
- Subject Access Request form
- Right to Erasure form
- HESA Student Collection Notice

Policy / procedure

1. Active data protection and information management

1.1. The OCA is registered with The Information Commissioner's Office and is entered on the Data Registry (reference Z7451677). Our Data Protection Officer can be contacted at dpo@oca.ac.uk.

1.2. Underpinning the commitment to responsible information management is a cycle of periodic data audits. These are major exercises, when all the individual pieces of data retained - and the processes adopted for managing them - are reviewed by senior managers.

2. Confidentiality and Non-disclosure Agreement

All OCA employees are required to agree to a Confidentiality and Non-disclosure Policy agreement. This sets out the need for confidentiality and makes explicit the serious consequences of any breach. In addition, the college's Email and Communications Policy sets out the responsibilities of all OCA Email account holders for ensuring the privacy and security of data shared via Email.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

3. Data security processes

3.1. OCA understands that it is critical to take steps to maintain the security of data received from students and employees in confidence. It has therefore defined detailed data security processes for obtaining, storing and disposing of confidential or sensitive data. As part of ensuring the college's processing of personal and sensitive data continues to remain secure, college employees are required as per its Data Protection Impact Assessment (DPIA) Policy to submit a DPIA Form for review and authorisation prior to any new data processing activities taking place.

3.2. The following IT and operational security procedures are operated by all employees:

- Adherence to the college's Network Security Policy to ensure that college systems and associated processes are not compromised or neglected.
- Ensuring continuous operations. There is a detailed Business Continuity Policy in place which encompasses:
- Disaster Recovery processes
- Secure, encrypted, data backup
- Secure offsite storage
- Data resilience
- Secure disposal.
- limiting the amount of paper-based, confidential or sensitive data held. Any necessary confidential or sensitive paper records are kept in secure storage in accordance with the college's Data Retention Schedule.

3.3. The following IT and operational security procedures are operated by all students:

- Adherence to the college's Student Computing Policy and associated policies to ensure security and integrity of the college's systems and platforms, in addition to ensuring the safeguarding of students and employees.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

4. Data Retention Schedule

4.1. Individual records are kept for as long as required – but no longer. As an HE provider, the Open College of the Arts is required to retain data for the purposes of meeting its statutory obligations to the Higher Education Statistics Agency (HESA), Her Majesty's Revenue & Customs (HMRC), the Office for Students (OfS), and the Quality Assurance Agency (QAA). These obligations are reflected through the college's Data Retention Schedule.

5. How do we store your data?

5.1. We store and process students' personal data in order to deliver our educational services to you in accordance with our Public Task in providing Higher Education Qualifications and allow operational teams to support you and conduct their duties.

5.2. We store and process employees' personal data to fulfil our contractual obligations and allow operational teams to support you and conduct their duties, and also for statutorily required purposes.

5.3. Personal and sensitive student data is securely shared with employees on a strictly confidential and need-to-know basis using the college's centrally managed systems. In the event that a student voluntarily discloses personal or sensitive data to an employee which they have not already disclosed to the college, it is the responsibility of the student to ensure that the college is given access to this data if it impacts upon their studies.

5.4. Special category data collected from you may be used to establish any additional support needs or reasonable adjustments required for you to succeed. This data may also be used by the college to identify groups of individuals not being reached by the college, and identify how it is being outwardly perceived.

5.5. We will apply analytical methods to your personal data and any volunteered student feedback to create an engaging online study environment which enhances progression and attainment.

6. Data processing partners

6.1. In order to provide its services to students and employees, the college selectively shares data with third party processing partners. Data is only shared with third party data processors where adequate protections have been established for that data.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

Processing partners (applicable to all OCA Students and Employees):

- Worldpay – By making payment using a debit or credit card for new courses, students' sensitive card data will be shared with our E-Merchant provider, Worldpay. All payment information is securely encrypted at rest and in transit.
- Amazon Web Services (AWS) - The college uses AWS for storage of static files, as well as server and database hosting, and therefore student and employee data is shared with AWS through those services. All services and servers in use through AWS are hosted within the EU in adherence with required data protection regulations and information security standards.
- Overt Software - Overt is a hosting provider for the college's OCA Learn VLE, requiring student and employees' personal data to be shared. Overt's servers are based within the EU and are in compliance with the college's Data Protection requirements and expectations.
- Brickfield Education Labs - Brickfield provides tools for use by the college within its VLE to establish and remedy accessibility issues within its courses in addition to providing alternative formats of files uploaded to the VLE. Employees' first name, last name and Email address are shared with Brickfield Education Labs for the provision of educational services provided. No student data is shared.
- Panopto - Panopto is a provider of video media hosting and capture services. Employees' and Students' first name, last name and Email Address are shared with Panopto for the provision of the service. The college's Panopto server is hosted in the EU through a separate Data Protection Agreement applying to OCA as a college within the UK or EU.
- UCA - as the college's awarding University, employees' and students' personal and sensitive data is shared with UCA for the purposes of providing UCA-hosted services and providing data for the University's HESA submission as part of statutory requirements. Data shared between OCA and UCA is held under the latter's Data Protection Policy.

- The Open University (OU) - OU, as the college's awarding University, employees' and students' personal and sensitive data is shared with OU for the purposes of providing OU-hosted services and providing data for the Open University's HESA submission as part of statutory requirements. Data shared between OCA and OU is held under the latter's Data Protection Policy.
- Open Athens - this service provides students on accredited programmes of study with access to UCA's online library. Personal data including full name, college Email account, programme of study and broad location (UK or Rest of World) is shared in order to provide the service. All employees are also provided access to the UCA online library through the same means, requiring the sharing of first name, last name, college Email account and Department with Open Athens.
- Mailchimp – your data (first name, surname, Email address, Programme of Study and Student Number) will be shared with Mailchimp, a USA-hosted service which applies data protection safeguards in line with the EU's Standard Contractual Clauses. Employees' first name, surname and college Email address are shared with Mailchimp for the sending of notices and to allow team members to conduct college business through the platform.
- Google – The Google Workspace for Education suite of cloud-based tools, including Email, Gdrive and other online services, are provided to all employees for the fulfilment of their duties and all students at the point of enrolment. To provide these services, students' personal data, including full name and programme of study at OCA, is used to create their accounts. All student and employee data is stored within the EU.
- Padlet - a Private instance of the Padlet application, used in various Academic Departments for collaborative sharing and aggregation of research. Student and employee personal data shared includes full name and college-issued email address.
- Twilio - an SMS service which the college makes use of to centrally issue prompts or updates to students.
- Zoom.us – a Video Conferencing service which enables employees and students to meet online virtually. A separate EU Data Protection Addendum containing EU Standard Contractual Clauses for the protection of data leaving the EEA has been established between the

college and Zoom.us, to account for its use of non-EEA-based servers.

- We share your data with funding providers, for example the Student Loans Company and the national funding authorities / government bodies e.g. Student Finance England, Wales and Northern Ireland.
- OCA is required to share student and employee data with the Higher Education Statistics Agency (HESA), and your contact details may be passed to survey contractors to carry out the National Student Survey (NSS), other surveys of students' views about their study, and surveys of student finances. This data may be provided directly by OCA or its parent University, the University for the Creative Arts for the purposes 1 and 2 outlined in HESA's Student Collection Notice.

Processing Partners (applicable only to OCA Employees):

- HMRC - for processing of employees' pay
- Barnsley Council - for managing secure access to the college's premises at DMC02 in Barnsley.
- UCA Payroll - Employees' sensitive financial information is shared with the UCA Payroll team for the processing of employee pay.
- Microsoft - All OCA employees are provided with Microsoft Office 365 accounts via their college-supplied Google Accounts. Data shared with Microsoft is limited to full name, department and college email address.
- Sage Finance systems - Flexible Tutors' financial information is securely stored by Sage for the processing of pay.
- Docusign - Employees' full name and email address is shared with Docusign for the purpose of providing contracts and requesting signed acceptance of those contracts.

7. Data Breach Policy

The college's Data Breach 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 and other college stakeholders to follow in the event of such a data breach occurring.

8. Subject Access requests

8.1. The UK Data Protection Act 2018 and EU GDPR give to you the right of access to the personal information OCA holds about you. You may send OCA a Subject Access Request (see 8.3) requiring OCA to tell you about the personal information OCA holds about you, and to provide you with a copy of that information.

8.2. OCA must respond to a valid subject access request within 30 calendar days of receiving it. OCA does not charge a search fee for providing this information, but in the event of manifestly unfounded, excessive or repetitive requests, a fee will be levied, based on the administrative cost of providing the information.

8.3. Subject Access Requests can be made through completion of the college's Subject Access Request form or in writing to the college's Data Protection Officer at dpo@oca.ac.uk including details of the information being requested, your full name and the format in which you wish to receive the response (digital or by post.)

9. Right to erasure

9.1. Data is retained by OCA in accordance with its published Data Retention Schedule, unless a Right to Erasure (see 9.6) is exercised within this time.

9.2. The College has statutory duties to the Higher Education Statistics Agency (HESA), Her Majesty's Revenue & Customs (HMRC), the Office for Students (OfS), and the Quality Assurance Agency (QAA) among others, to report, process, and keep data for specified periods that supercede the Right to Erasure. The College's Data Retention Schedules are considered with these obligations in mind.

9.3. OCA has one calendar month to respond to the request. In certain circumstances, extra time may be required to consider the request, up to an additional two months. In the event that an extension beyond one calendar month is required, the college will inform the data subject within one month that more time is needed and the reasons why. For more on this, see the ICO guidance on time limits.

9.4. OCA may require the data subject to prove their identity. In such cases, the one-month time period to respond to the request begins from when the college receives this additional information.

9.5. In most circumstances, no fee is charged.The college can only charge a fee if the request is 'manifestly unfounded or excessive'. A reasonable fee for administrative costs associated with the request may in such exceptional cases be requested.

9.6. Requests for data to be erased can be made to any employee of the college, verbally or in writing. You can also submit the college's Data Erasure form, or make a direct request to the college's Data Protection Officer in writing at dpo@oca.ac.uk.

9.7. OCA can refuse to erase the data in the following circumstances:

- When keeping the data is necessary for reasons of freedom of expression and information (this includes journalism and academic, artistic and literary purposes).
- When OCA is legally obliged to keep hold of your data such as to comply with financial or other regulations.
- When OCA is carrying out a task in the public interest or when exercising their official authority.
- When keeping the data is necessary for establishing, exercising or defending legal claims.
- When erasing the data would prejudice scientific or historical research, or archiving that is in the public interest.

9.8. The right to erasure also does not apply to special category data in the following circumstances:

- When keeping hold of the data is necessary for reasons of public health.
- When keeping the data is necessary for the purposes of preventative or occupational medicine. This only applies if the data is being used by or under the responsibility of a professional who is under a legal obligation of professional secrecy, such as a health professional.

9.9. If an exemption applies, OCA can either fully or partly refuse to comply with the request.

OCA can also refuse the request if it is, as the law states, '*manifestly unfounded or excessive*'.

There is no set definition of what makes a request 'manifestly unfounded or excessive'. It depends on the particular circumstances of the request. For example, an organisation may consider a request to be 'manifestly unfounded or excessive' if it is clear that it has been made with no real purpose except to cause the organisation harassment or disruption.

In such circumstances OCA can:

- request a reasonable fee to deal with the request; or,
- refuse to deal with the request.

In either case OCA will need to inform the data subject making the request and justify the decision.

9.10. If, having considered the request, OCA decides it does not need to erase the data, the college will still respond to the data subject with its justification, together with details of their right to complain about this decision to the ICO, or through the courts.

9.11. If, having considered the request, OCA decides that no exemption applies, OCA will delete the data it holds on the data subject.

9.12. OCA will also request for any data processors the subject's data has been shared with to also delete any data held on the data subject. The college can only refuse to do this if it would be impossible or involve disproportionate effort. If you ask, OCA must also inform you that they have shared their data with other organisations.

9.13. If the subject's data has been made public online - such as on social networks, forums or websites - then OCA must take reasonable steps to inform those with responsibility for these sites to erase links or copies of that data.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

10. Right to restriction

10.1. Any individual with either current or past interaction with the college has the right to request that either the processing or scope of their data held by the college be restricted.

10.2. Where the college has no legal or contractual basis for the processing or storage of that data, the request will be processed and the outcome communicated to the individual.

10.3. Where the college has a legal or contractual basis for the processing or storage of that data, the reason for rejection of the request will be communicated to the individual, referencing the college's Complaints Policy and the ICO complaints process.

10.4. Requests for restriction of data processing and storage can be made in writing to the college's Data Protection Officer at dpo@oca.ac.uk.

11. Right to rectification

11.1. Any student or employee has the right to request that any inaccurate or incomplete data held by the college be rectified.

11.2. Employees requesting that their data be rectified should make their initial request through their line manager, who will either action the request or ensure the request is appropriately processed.

11.3. Students' requests can be made by filling in the Student Change of Details form.

12. Right to portability

12.1. Either during or immediately following the conclusion of a student or employee's involvement with the college, they may, within the allowances of the Data Retention Schedule, request their data to be supplied to them in a non-proprietary and accessible format.

12.2. As part of a student's withdrawal, completion or other termination of studies, the opportunity for them to obtain their data in a portable format must be provided prior to revocation of access to systems which hold that data.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

12.3. In the event of the termination of an employee's contract, the opportunity for them to obtain their data in a portable format must be provided prior to revocation of access to systems which hold that data.

12.4. Requests for data can either be made directly through services provided in the case of: Google Workspace; OCA Learn; Padlet and OCA Spaces, and/or by making the request in writing to the college's Data Protection Officer at dpo@oca.ac.uk.

13. Right to object

13.1. You have the right to object to the processing of your personal data where you believe there to be either an inaccuracy in the data, or that the data is being unlawfully processed.

13.2. Where your rights are deemed to override the lawful basis by which the college processes your data, the request will be processed and the outcome communicated to you.

13.3. In the event that following the processing of your request the college arrives at the decision that the college can continue to process your data, the decision for rejection of the request will be communicated to you, referencing the college's Complaints Policy and the ICO complaints process.

13.4. Objections can be made in writing to the college's Data Protection Officer at dpo@oca.ac.uk.

14. Exercising your rights

14.1. In addition to any of the means specified above, you may exercise your rights through any of the following channels:

- By post: Open College of the Arts, The Michael Young Arts Centre, Room 201, DMC02, County Way, Barnsley, S70 2AG
- By phone: +44 (0)1226 978330
- By Email: dpo@oca.ac.uk

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Board	6 July 2022	1 June 2023

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; all students and employees are covered by this policy.

Non-Compliance

Any student or employee found to be non-compliant with this policy may face repercussions, up to and including termination of enrolment or 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 alternatively your own line manager, or other management employee for advice.