Open College of the Arts
Data Protection and Confidentiality Policy

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

The objectives of the Data Protection and Confidentiality 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.

There are seven principal components to the policy:

- Active data protection and information management
- Confidentiality and Non-disclosure Policy
- Data security processes
- Student records retention schedule
- Data processing partners
- Data Breach policy
- Subject Access Requests
- Right to Erasure

1. Active data protection and information management

The OCA is registered with The Information Commissioner's Office and is entered on the Data Registry (reference Z7451677). Stephanie Gillott (Academic Registrar) is the nominated Data Controller.

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 Policy

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** [www.oca.ac.uk/about-oca/policies/] sets out the responsibilities of all OCA Email account holders for ensuring the privacy and security of data shared via Email.

3. Data security processes

OCA understands that it is critical to take steps to maintain the security of data received from students and tutors 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** [www.oca.ac.uk/about-oca/policies/] to submit a DPIA Form for review and authorisation prior to any new data processing activities taking place.

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

- Adherence to the college's **Network Security Policy** [www.oca.ac.uk/about-oca/policies/] 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** [www.oca.ac.uk/about-oca/policies/].

4. Data Retention Schedule

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. Data processing partners

In order to provide its services to students, tutors and staff, 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.

In order for the college to fulfil its duties as an education provider, it employs the services of the following Data Processing partners:

- Worldpay – By making payment using a debit or credit card for new courses, your sensitive card data will be shared with our E-Merchant provider, Worldpay through one of its sub-companies, CardSave. All payment information is securely encrypted.
- Amazon Web Services (AWS). The college uses AWS for storage of static files, as well as server and database hosting.
- Overt Software. Overt are a hosting provider for the college's OCA Learn VLE. Overt's servers are based within the EU and are in compliance with the college's Data Protection requirements and expectations.
- UCA - as the college's parent University, students' personal and sensitive data is shared with UCA for the purposes of providing UCA-hosted services and providing data for the University's annual HESA submission as part of statutory requirements. Data shared between OCA and UCA is held under the latter's Data Protection Policy.
- Open Athens - this services 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.
- Mailchimp – your data (first name, surname, Email address) will be shared with Mailchimp, a USA-hosted service which applies data protection safeguards in line with the EU-US Privacy Shield Framework.
- Google – The G-suite for Education suite of cloud-based tools, including Email, Gdrive and other online services, are provided to 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 G-suite accounts.
- OCA tutors operate on a contractual basis for the college and are therefore classed as a processing partner. Personal and sensitive data is securely shared with tutors on a strictly confidential basis using the college's centrally managed systems.
- Twilio - an SMS service which the college makes use of to centrally issue prompts or updates to students. This service applies data protection safeguards in line with the EU-US Privacy Shield Framework.
- Zoom.us – a Video Conferencing service which enables staff, students and tutors to meet online virtually. A separate EU Data Protection Addendum has been established between the college and Zoom.us, to account for its use of non-EU-based servers.

For college tutors to fulfil their roles, it is necessary for the college to share students' personal and in some cases sensitive data with their tutor. In the event that a student voluntarily discloses personal or sensitive data to a tutor 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.

6. Data Breach Policy
The college's **Data Breach Policy** [www.oca.ac.uk/about-oca/policies/] 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.

7. Subject Access Requests
The General Data Protection Regulation (GDPR) gives to you the right of access to the personal information OCA holds about you. You may send OCA a **Subject Access Request** (see Links) requiring OCA to tell you about the personal information OCA holds about you, and to provide you with a copy of that information.

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. Right to Erasure
Data is retained by OCA for the full duration of students' studies, plus six calendar years, unless a Right to Erasure (see Links) is exercised within this time. 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. The College Data Retention Schedules are considered with these obligations in mind.

Links
Email and Communications Policy: https://www.oca.ac.uk/about-oca/policies/
Data Protection Impact Assessment (DPIA) Policy: https://www.oca.ac.uk/about-oca/policies/
Network Security Policy: https://www.oca.ac.uk/about-oca/policies/
Data Retention Schedule: https://www.oca.ac.uk/about-oca/policies/
Data Breach Policy: https://www.oca.ac.uk/about-oca/policies/
Data Breach Report Form: https://goo.gl/forms/D7rt3rfBBISVYwl82
Freedom of Information Request form: https://goo.gl/forms/tdXphRhiLfY0CFee2
Right to Erasure form: https://goo.gl/forms/Soi6IhD18w8h0Rk53