Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

OCA Data Protection Policy

Purpose

This policy is intended to ensure that personal information is collected and used in compliance with the UK General Data Protection Regulation (the “UK GDPR”) and other related legislation.

The policy sets out the requirements that must be adhered to when processing personal data, delivering the OCA’s commitment to protecting the rights and privacy of individuals by safeguarding their personal data and ensuring that privacy is central to what we do.

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

Scope

This policy applies to all personal data, including special categories of personal data,

processed by the Open College of the Arts (OCA).

This includes all electronic personal data, and any other personal data which has some form of structure or index enabling the relevant information to be located. It applies to data in any medium or format, including but not limited to, data stored on electronic media, transmitted across networks, printed out or written on paper, or spoken over a

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

communications medium (e.g., Cellular). This policy applies regardless of where the personal data is held, including outside the OCA property and on personally owned equipment or in personal accounts.

This policy applies to everyone working for or on behalf of the OCA who obtains, uses, accesses or stores personal data, regardless of their role, grade or type of contract. This includes, but is not limited to, agency staff, consultants, volunteers, visiting research and teaching staff and external committee members. It also applies to all students when processing personal data on behalf of the OCA or as a requirement of their studies; and anyone who accesses OCA systems, including suppliers and contractors.

Changes

This is the first version of this standalone Data Protection Policy, which has been extracted from the previous 'Data Protection and Confidentiality Policy' as part of its annual review.

Privacy-related aspects including data processing partners have been moved to their own Data Privacy Policies for their respective audiences.

Standards previously incorporated into the Data Protection and Confidentiality Policy have been moved to a separate Data Protection Standard.

Policies superseded by this document

Data Protection and Confidentiality Policy, version 4, 10/01/23

Related policies and legislation

This policy references:

- UK Data Protection Act 2018
- EU GDPR 2018
- Student Computing Policy
- Information Security Policy Set
- Data Protection Impact Assessment (DPIA) Policy
- Data Retention Schedule
- Data Breach Procedure

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

- Data Breach Report Form
- Subject Access Request form
- Right to Erasure form
- HESA Student Collection Notice
- Prevent Policy
- Safeguarding Policy

Introduction

The OCA collects and uses personal data relating to various categories of individuals, including enquirers, students, alumni, informal learners, members of staff, volunteers, research participants, employees of partner and supplier organisations, and anyone who communicates with the OCA. The purposes for processing this personal data are set out in the OCA's privacy notices. The OCA is subject to the UK GDPR and the UK Data Protection Act 2018, the Privacy and Electronic Communication regulation 2003, and associated legislation. The OCA is registered with the UK Information Commissioner's Office (ICO) as a data controller (Z7451677).

Definitions

Definitions of terms are those used in the UK GDPR.

Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

Policy:

1. Data protection principles

The College ensures that personal data is processed in compliance with legislation by setting out rules and processes in the Data Protection Standard. The legislation sets out the following principles that all processing of personal data must adhere to.

Personal data will be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- (“lawfulness, fairness and transparency”)
- collected and created for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”)
- adequate, relevant and limited to what is necessary in relation to those purposes (“data minimisation”)
- accurate and, where necessary, kept up to date (“accuracy”)
- retained for no longer than is necessary (“storage limitation”)
- kept safe from unauthorised access, accidental loss or deliberate destruction (“integrity and confidentiality”)

2. Special category data

The OCA ensures additional controls are in place for “special category” (sensitive) personal data, and personal data concerning criminal convictions. This is because use of this data could create significant risks to the individual’s fundamental rights and freedoms.

Special category data is set out in the UK GDPR as follows:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person’s sex life;
- data concerning a person’s sexual orientation.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

Personal data relating to criminal conviction and offences includes data about criminal activity, allegations, investigations, and proceedings. It includes information relating to the absence of convictions, personal data of victims and witnesses of crime, data about penalties, and conditions or restrictions placed on an individual as part of the criminal justice process.

The processing of special category personal data, and personal data relating to criminal convictions, must comply with the data protection standard, which sets out specific safeguards for special category and criminal conviction data in order to comply with the principles of the GDPR and UK GDPR.

Processing of data relating to criminal convictions must only be carried out where there is a basis in the legislation to do so.

All processing of special category data must be noted in our Record of Processing Activity, along with the basis for processing it and its retention period.

3. Data subject rights

OCA will uphold individual data subject rights, specifically the right to:

- obtain free of charge, confirmation as to whether personal data concerning them is being processed and, if it is, a copy of that personal data
- have their personal data rectified and incomplete personal data completed
- erasure when no longer required or to be forgotten, subject to legal obligations
- object to and restrict further processing of their data until the accuracy of the data or use has been resolved
- data portability where the personal data has been provided by consent or contract for automated processing and the data subject requests that a machine-readable copy be sent to another data controller
- not be subject to a decision based solely on automated decision making and processing

We will communicate these rights to data subjects through timely privacy notices.

4. Accountability

OCA is accountable to the principles above, and so will ensure that

- privacy notices are maintained, to inform individuals as to the purposes and means of processing their information

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

- where possible, the quality and accuracy of information processed is periodically confirmed, and there are mechanisms for data subjects to update their data.
- personal data is regularly reviewed and destroyed, according to the retention schedule, to ensure that is not held longer than is necessary
- personal data is shared only where is it necessary and appropriate to do so, and that data sharing agreements and data processor agreements are in place where necessary to protect the information
- Appropriate security measures are in place to safeguard personal data, via information security policies and other mechanisms
- Personal data breaches, incidents, and near misses are documented and tracked, and reported to the regulator where necessary
- Data subject rights are fulfilled appropriately, and within the necessary timescales
- Data protection by design is carried out for new activities and where processing changes, including the completion of Data Protection Impact Assessments
- Our personal data processing activities are documented, and regularly reviewed and kept up to date
- The data protection standard is maintained, setting out the specific responsibilities and activities required to maintain compliance
- Overall compliance with the legislation is monitored by the Data Protection Officer

Responsibilities

Users of the college's personal data must:

- Comply with the requirements of the Data Protection Standard, in order to adhere to the data protection principles and protect individuals' rights and freedoms in respect of their personal data.
- Complete relevant training to support compliance with this policy and the associated standard.
- Engage with and follow processes as set out in the Standard in a timely way.

The Data Protection Officer is responsible for assessing the compliance of the college and advising the Information Risk Owner and colleagues on compliance risks and issues.

I.T Services Team are responsible for conducting security risk assessments, carrying out vulnerability scans, managing security incidents, maintaining and communicating information security policies, and advising staff on security issues

Heads of Departments/ Information Asset Owners have overall responsibility for the processing of personal data and for monitoring compliance within their areas of responsibility, and as such, are information asset owners. They are responsible for

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

ensuring that the personal data in their area of responsibility is processed in compliance with the data protection standard. They are also responsible for ensuring that all staff, volunteers, consultants, research students and individuals that are associated with their unit are aware of the policy and standard, have received appropriate training, and have necessary resources and equipment to comply with the Policy and Standard.

Non-Compliance with this Policy

In addition to this Data Protection Policy the Data Protection Standard shall be adhered to and applied across all projects, programs, systems and/or initiatives.

Where users cannot adhere to the data protection standard for any reason, an exception should be raised as set out in the standard.

Any careless or deliberate infringement of this policy, the Data Protection Standard, or data protection law by users of personal data will be treated seriously by the college and may result in disciplinary action.

The responsibilities outlined in this policy do not waive personal liability for individual criminal offences resulting from the wilful misuse of personal data under data protection law. These include:

- Unlawfully obtaining, disclosing or retaining personal data
- Re-identifying de-identified personal data without the authority of the data controller or processor
- Altering or deleting personal data to prevent disclosure in accordance with the rights of access to data subjects
- Impeding an officer of the Information Commissioner's Office in the course of their duty

Review and Monitoring

The Policy will be reviewed annually or wherever necessary as part of legislative or organisational change. This is to ensure that it remains effective and compliant with relevant legislation.

If the Policy is updated then the Standard, as well as all other data protection and privacy documentation, controls and processes must be reviewed, and where necessary, updated, to ensure alignment

The Policy will be reviewed by the; Head of Technology and Innovation and approved by the Group Data Protection Officer.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
1	Approved	Paul Vincent	Will Woods		01/08/24

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.