Data Protection Policy

August 2025

1. Policy Summary

1.1. 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.

1.2. 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.

2. Scope

2.1. What does this policy cover?

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

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

2.1.3. 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 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.

2.1.4. 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.

3. General Principles

3.1. 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

3.1.2. Example

4. Data protection principles

4.1. 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.

4.2. 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”)

5. Special category data

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

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

5.6. 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.

6. Data subject rights

6.1. 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

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

7. Accountability

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

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

7.1.2. where possible, the quality and accuracy of information processed is periodically confirmed, and there are mechanisms for data subjects to update their data.

7.1.3. personal data is regularly reviewed and destroyed, according to the retention schedule, to ensure that is not held longer than is necessary

7.1.4. 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

7.1.5. Appropriate security measures are in place to safeguard personal data, via information security policies and other mechanisms

7.1.6. Personal data breaches, incidents, and near misses are documented and tracked, and reported to the regulator where necessary

7.1.7. Data subject rights are fulfilled appropriately, and within the necessary timescales

7.1.8. Data protection by design is carried out for new activities and

where processing changes, including the completion of Data Protection Impact Assessments

7.1.9. Our personal data processing activities are documented, and regularly reviewed and kept up to date

7.1.10. The data protection standard is maintained, setting out the specific responsibilities and activities required to maintain compliance

7.1.11. Overall compliance with the legislation is monitored by the Data Protection Officer

8. Responsibilities

8.1. 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.

8.2. **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.

8.3. **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

8.4. **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 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.

9. Non-Compliance with this Policy

9.1. 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.

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

9.3. 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.

9.4. 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

10. Review and Monitoring

10.1. 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.

10.2. 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

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

11. Glossary of terms

11.1. Data Controller

The entity that determines the purposes and means of processing personal data.

11.2. Data Minimisation

A principle requiring that the personal data processed should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

11.3. Data Portability

The right to receive the personal data concerning oneself, which one has provided to a controller, in a structured, commonly used, and machine-readable format and the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

11.4. Data Processing

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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

11.5. Data Protection Officer (DPO)

A person appointed to ensure an organization complies with the GDPR, to inform and advise on data protection obligations, to monitor compliance, and to be the point of contact for data subjects and the Information Commissioner's Office (ICO).

11.6. General Data Protection Regulation (GDPR)

EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

11.7. Lawfulness, Fairness, and Transparency

A principle requiring personal data to be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

11.8. Personal Data

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.

11.9. Purpose Limitation

A principle that personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

11.10. Storage Limitation

11.11. A principle that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

11.12. Subject Access Request (SAR)

The right of individuals to access personal data held about them and to obtain information about how it is processed.

11.13. Special Category Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

11.14. **Accountability**

A principle that requires data controllers to be responsible for and be able to demonstrate compliance with the GDPR.

11.15. Integrity and Confidentiality (Security)

A principle that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

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 alternatively 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. Student Computing Policy

13.4. Information Security Policy Set

13.5. Data Protection Impact Assessment (DPIA) Policy

13.6. Data Retention Schedule

13.7. Data Breach Policy

13.8. Data Breach Report Form

13.9. Subject Access Request form

13.10. Right to Erasure form

13.11. HESA Student Collection Notice

13.12. Prevent Policy

13.13. Safeguarding Policy

14. Changes since previous policy

14.1. Updated to use the college's new Policy Template.

14.2. Removed references to previous validating University (the University for the Creative Arts)