Royal College of Art
Postgraduate Art & Design

Vice-Chancellor's Office Data Protection Policy

CATEGORIES

IT Services

The Royal College of Art (the College) processes the personal data of staff, students and other individuals who come into contact with the College. This information is gathered in order to enable the provision of education and other associated functions. In addition, the College may be required by law to collect, use and share certain information.

The College is registered as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website:

RCA registration number: Z5688595
EXPIRES: 28 October 2019

The College issues has a series of Fair Processing Notices for Staff, Students and Alumni. These details the purpose of processing personal data as well as the legal bases that they rely on.

All data kept within the College that falls within the General Data Protection Regulation (GDPR) is recorded in the central Information Asset Register and associated Retention Schedule.

Purpose

This policy sets out how the College deals with Personal Data correctly and securely and in accordance with the GDPR, and other related legislation.
All College staff and regulators involved with the collection, use, processing or disclosure of Personal Data will be aware of their duties and responsibilities and will adhere to this policy.

Personal data only includes information relating to natural persons who: can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. Examples include an individual's name, address, date of birth or photograph.

Personal Data may also include special categories of information such as trade union affiliation, criminal conviction and offences or biometrics. These are considered to be more sensitive and the College may only process them in more limited circumstances.

Commitment

The College is committed to maintaining the above principles at all times.
Therefore, the College will:

1. Inform individuals why Personal Data is being collected;
2. Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this;
3. Check the accuracy of the information it holds and review it at regular intervals;
4. Ensure that only authorised personnel have access to the Personal Data whatever medium (paper or electronic) it is stored in;
5. Ensure that clear and robust safeguards are in place to ensure Personal Data is kept securely and to protect Personal Data from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
6. Ensure that Personal Data is not retained longer than needed;

7. Ensure that when Personal Data is destroyed it is done so appropriately and securely;
8. Share Personal Data with others only when it is legally appropriate to do so;
9. Comply with the duty to respond to requests for access to Personal Data, known as Data Subject Access Requests (DSARs);
10. Ensure that Personal Data is not transferred outside the EEA without the appropriate safeguard;
11. Ensure all staff and governors are aware of and understand these policies and procedures.

Policy

Information Systems Security Policy - Supporting Policy 1: Compliance with the Data Protection Act (2018).

The College must, in the course of its operation collect Personal Data about its members of staff, contractors, students, and other users to allow it to monitor compliance, performance, health and safety and security.

In managing data, the College will adhere to the data protection principles prescribed by current Data Protection legislation, and associated regulations.

It is a requirement of the GDPR and the Data Protection Act, 2018 that the College is responsible for, and can demonstrate compliance with the data protection principles, rights and requirements for processing Personal Data. It is a condition of ongoing engagement with the College, that all personnel, regardless of status, must comply with the provisions of this policy. Everyone involved with the College has a responsibility to protect the Personal Data of individuals that interact with the College.

Whenever there has been an actual or suspected change to the risk to individuals' rights and freedoms with respect to data privacy, a Data Privacy Impact Assessment (DPIA) will be completed and assessed by the Data Protection Officer. A DPIA will also be assessed prior to any new or amended processing of Personal Data, where it is deemed appropriate.

Breaches of the Policy

All College personnel are expected to be vigilant to the possibility of breaches of this policy and of the GDPR. Personnel who become aware of, or suspect such a breach must report it immediately to the Data Protection Officer.

Introduction

It is a requirement of the GDPR that Personal Data must be held and processed securely and this is a component of the College's Data Protection policy, the full details of which may be found on the College Website. The processing of Personal Data, in the College has to be registered with the College Data Protection Officer. In accordance with the GDPR, Personal Data has to be handled in compliance with a set of seven principles. The Act also gives rights to individuals about whom data is held (Data Subjects) which must be observed.

Registration/Notification

Any Personal Data held on computer, or manually in relevant structured files, as defined in the GDPR, may be processed for a particular purpose only if that purpose has first been registered with the College Data Protection Officer, and subsequently notified to the Information Commissioner. Where a user downloads Personal Data from a database for his/her own use, this constitutes a new database and must be registered accordingly. The College is also required to lodge with the Commissioner the details of the systems it has put in place to ensure the security of Personal Data held on those databases.

Compliance with the Data Protection Principles

The GDPR establishes seven principles that must be adhered to at all times:

1. Personal Data is processed lawfully, fairly and in a transparent manner in relation to the data subject;
2. Personal Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Personal Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);

4. Personal data is accurate and where necessary, kept up to date; every reasonable step is taken to ensure that Personal Data that are inaccurate are erased or rectified without delay;
5. Personal Data is 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;
6. Personal Data is protected by implementing adequate security by means of 'appropriate technical and organisational measures';
7. The College takes full accountability for what it does with Personal Data and how it complies with the above principles.

The College maintains appropriate measures and records which allow it to demonstrate its compliance with these principles.

Data Security

Ensuring that personal data is held securely is a key feature of the GDPR. Personal Data should not be disclosed either orally or in writing or accidentally to any unauthorised third party. If computerised, it should be protected by password, encryption or firewall according to sensitivity or kept only on a disk which is itself kept securely. Unauthorised disclosure will usually be considered a disciplinary matter and may be considered gross misconduct in some cases.

CCTV

The College has a separate policy dedicated to the regulatory requirements and procedures for monitoring and managing its CCTV installation and the data captured. The CCTV Policy is owned by Buildings & Estates.
It is the RCA's policy, whenever CCTV is in use, to ensure that:

- Individuals are aware that they are being recorded;
- They understand the reasons why they are being recorded;
- There are defined retention periods for all recordings; and
- Individuals know how they can obtain access to recordings through a Data Subject Access Request.

Data Subject Access Requests (DSARs)

In accordance with the GDPR, a Data Subject is entitled to be given a description of the types of their Personal Data being processed by the College, how the Personal Data was acquired, how and why it is being processed, how it will be disposed of, and if applicable, who it is shared with. The term 'processed' in this context is very broad and includes all uses and storage means.

A Data Subject also has a right to see the actual data held.

It is important to recognise that there is no specific form in which a DSAR has to be made, including verbally. In almost all cases DSARs must be processed without charging the Data Subject a fee.

The processing of a DSAR must not result in the disclosure of Personal Data relating to another individual. Where Personal Data is mixed with other non-relevant Personal Data, the non-relevant Personal Data must be permanently redacted prior to disclosing the records.

When setting up and using databases of Personal Data, users must register the new database with the College Data Protection Officer and act in compliance with the Data Protection Principles to ensure that Personal Data is held and processed securely and the rights of the individual are preserved.

Complaints

Complaints will be dealt with in accordance with the College's complaints policy. Complaints relating to the handling of Personal Data may be referred to the Royal College of Arts Data Protection Officer who may be contacted at:

dpo@rca.ac.uk
Royal College of Art
Kensington Gore
London SW7 2EU

Or to the Information Commissioner who can be contacted at: Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at; www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every three years. The policy review will be undertaken by the Chief Operating Officer (COO), or a nominated representative.