Royal College of Art

Data Protection Policy

Version	Final
Date	June 2023
Reviewed	No less frequently than every 3 years.
Approved by	SMT
Target audience	All staff
Cascaded to	All staff via intranet
Policy Lead	Alex Smith alex.smith@rca.ac.uk
Owner	Data Protection Officer
Department	VCO & Governance
Equality Impact Assessment completion	29/06/2023

Contents

Further links to information can be found in guidance boxes throughout the policy.

Purpose and Scope

The Royal College of Art ‘the College’ is committed to meeting its obligations under UK GDPR, the Data Protection Act 2018 and relevant legislation relating to protecting rights and freedoms of individuals and their information.

This policy has been established to ensure that the College and its staff comply with Data Protection law(s).

All staff must familiarise themselves with this policy and follow its guidance when processing personal data on behalf of the College.

Responsibilities

Staff

All staff are responsible for handling personal data in compliance with UK data protection laws on behalf of the College as the Data Controller.

Staff should:

- Make themselves familiar with this policy,
- Complete the mandatory GDPR training,
- Report any data breaches to the DPO using the data breach form .

Data Governance Network

The Data Governance Network identifies local roles across the College that support teams with data protection compliance and information risk management. You can read more about these roles and the network of people on the RCA intranet.

Data Governance Working Group

The Data Governance Working Group oversees data governance compliance risk for the College.

GDPR mandatory training is found on Moodle (https://moodle.rca.ac.uk). Go to Staff Training> HR and Mandatory Training > Staff Training> GDPR

Data breach reporting process is on the RCA intranet: https://intranet.rca.ac.uk/data-breach-management-procedure/

Data Protection Principles

Staff are required to adhere to processing personal data following the UK GDPR data protection principles. Principles are followed unless a legislative exemption is identified.

Principle a: Data is processed lawfully, fairly and in a transparent manner

- Personal data is only collected with a lawful basis as set out by the Data Protection Act 2018.
- All use of personal data requires a Privacy Notice that informs the individual about how their data will be used.
- Personal data is used within existing laws and consideration is given to the fairness of the processing on behalf of the individual in relation to their rights.

Principle b: Data is processed for specified, explicit and legitimate purposes

- Personal data is collected for an explicit purpose, as stated in a Privacy Notice.
- Personal data is not collected for reasons outside of the explicit purpose given.
- If new processing takes place, Privacy Notices are updated and re-published to data subjects.

Principle c : Data is adequate, relevant and limited to what is necessary

- Personal data processed is sufficient to properly fulfil the stated purpose,
- Personal data collection is limited to what is necessary for that purpose.

Principle d: Data is accurate and kept up to date

- Personal data is accurate and kept up to date,
- Where possible, opportunities are provided to individuals to update their data.

Principle e: Data is kept for not longer than necessary

- Personal data is stored in line with the College retention periods and is destroyed or deleted when no longer needed.

Principle f: Data is kept secure, confidentially and with integrity

- Personal data is held with appropriate security levels combining organisational and technical security measures to protect assets against unauthorised processing, loss, destruction and damage.

Accountability principle: Data is managed with accountability

- The College has an appointed Data Protection Officer (DPO) and a Senior Information Risk Owner (SIRO).
- All staff must complete GDPR mandatory training.
- Staff manage personal data responsibly and breaches are reported to the DPO.
- The College and its staff maintain records that evidence accountability including: Privacy Notices, records of consent, Data Protection Impact Assessments, data sharing agreements and contracts. The College maintains a Record of Processing Activity.

College Commitments

The College is committed to maintaining compliance with Data Protection law(s) at all times. Therefore, staff will:

1. Inform individuals why and how personal data is being processed and under what lawful basis it is being processed;
2. Report incidents to IT Services and the DPO immediately when a personal data breach has been discovered;
3. Ensure that any personal data is securely held, that it is accurate, up to date and not shared with unauthorised third parties;
4. Ensure that personal data is not held for longer than necessary, following the College's retention schedule where appropriate;
5. Comply with individual rights requests and forward them onto dpo@rca.ac.uk promptly where they cannot be completed by the recipient;
6. Meet the 'data minimisation' principle by processing a single source of personal data where possible;
7. Ensure all staff and governors are aware of and understand the Data Governance Framework and relevant policies;
8. Maintain a Record of Processing Activity ensuring that a valid legal basis is identified for all processing of personal data;
9. Ensure that personal data is not transferred to restricted countries without appropriate safeguard;
10. Ensure that when personal data is destroyed, it is done so appropriately and securely;
11. Comply with all data protection principles.

Data protection by Design and Default

The College is committed to data protection by design and default which embeds privacy into every aspect of processing personal data.

Collecting new data

- Before collecting or creating new personal data, staff will consider the impact its use could have on the rights and freedoms of individuals. Personal data being created or collected will be described in a Privacy Notice shared with data subjects.
- If you intend to:

  · Conduct systematic and extensive profiling,
  · Process special category data on a large scale,
  · Systematically monitor a public area,

  You must complete a Data Protection Impact Assessment to be reviewed by the Data Protection Officer to assess risk and implement risk mitigation strategies.

Information on Privacy Notice and Data Protection Impact Assessments, including templates, can be found on the RCA Intranet: https://intranet.rca.ac.uk/data-protection-info/

Systems & Network Security

- All personal data is held on College systems within the College IT network. These systems are secured using security measures managed by ILTS.
- Staff must follow Information Security policies to maintain security, particularly where personal devices are used. Staff must complete mandatory IT Security training.
- Systems and applications containing personal data will be administered by default to keep information secure so that data will have restricted and managed access.
- Personal data should not be disclosed to any unauthorised third party. Requests for data that are not authorised within existing procedures should be assessed by the DPO before disclosure.

Physical Security

- Physical access to buildings or areas where data is stored are locked, secure and monitored.
- Staff should avoid processing personal data in public spaces and where it's necessary should ensure the privacy of personal data in these spaces following the IT Security Policy.

Sharing data internally

- Personal data should not be shared using email attachments, additional protections should be used for special category data.
- Personal Data in management reports should be anonymized where possible.
- Staff should access and store personal data on centralised records (Thesis, iTrent, Raiser's Edge) wherever possible.
- Staff finance data can be internally shared confidentially with specific, named Research Office staff for the purpose of accurate bid grant submissions and for reporting and reconciliation of post-award work.
- In other situations where data protection laws are used to prevent internal data sharing, the DPO will advise best practice.

Sharing with third parties

The College is responsible for any personal data processing that is outsourced or shared with subcontractors or 3rd party businesses.

- Staff members using a third party for personal data processing should have a contractual agreement in place that includes data protection clauses. The clauses will instruct the contractor on how to process the College's data as well as other legal obligations it has relating to the College's data.
- Staff setting up a partnership with another organisation that involves sharing or collecting personal data will need a Data Sharing Agreement. The Data Sharing Agreement describes the lawful responsibilities of each party in relation to the data.
- Staff members asked to share personal data with government authorities (such as police or agencies) with no agreement in place, the College will rely on a legal obligation to disclose or there must be a valid exemption under the Data Protection Act 2018. Staff should seek the advice of the Data Protection Officer for this type of sharing where it is outside of usual procedure.

Contact the Data Protection Officer to discuss your data sharing at dpo@rca.ac.uk

International transfers

- Staff must ensure that international transfers of personal data have appropriate safeguards in place.
- Data is not transferred to countries that are not deemed adequate without safeguards, such as contractual clauses within transfer agreements.

You can find the International Data Transfers FAQs on the intranet.

https://intranet.rca.ac.uk/data-protection-info/

Research Data Management

- Principal investigators and staff conducting research should follow the Research Data Management Policy.

You can find guidance on managing research data on the intranet.

https://intranet.rca.ac.uk/research-knowledgeexchange/research-staff/research-data-management/

Data Breaches

- Personal data breaches or incidents must be reported to IT and the Data Protection Officer on discovery.
- The College is obligated to report serious breaches to the Information Commissioner's Office within 72 hours of discovery.
- Additional staff training may be required in response to breach incidents.

Staff can report breaches using the Data Breach form on the RCA intranet.

https://intranet.rca.ac.uk/data-breach-management-procedure/

Individual Rights

All individuals are entitled to exercise their rights under Data Protection laws. Individual Rights can crossover with day to day business activities undertaken by the College. Staff should be aware of these rights, and understand they can be requested verbally. The rights may not apply in all cases; where responsibility of the College is unclear the Data Protection Officer should advise.

The College will respond to requests within 1 calendar month, in exceptional circumstances this may be extended to 2 months.

The Individual Rights are:

1. The Right to be informed (fulfilled by a Privacy Notice)
2. The Right of access (providing copies of personal data to the data subject)
3. The Right of rectification (amending incorrect records)
4. The Right to erasure (deleting records)
5. The Right to restrict processing (limit the way data is used)
6. The Right to data portability (disclose data to third parties)
7. The Right to object (stop using data)
8. Rights in relation to automated decision making (human review of automated decisions)

‘Subject Access Requests’, requests for large sets of data, or large data deletions should be promptly sent to dpo@rca.ac.uk for handling.

Breach of Policy

If personal data is used in a way that does not follow this policy it should be reported to dpo@rca.ac.uk. You can also contact the College Secretary to report misuse under the Whistleblowing Procedure.

Breaches may require additional training for staff. Serious misuse or breaches (such as flagrant or purposeful unauthorised disclosure) of this policy may constitute gross misconduct in which case disciplinary procedures can be instigated.

Related Legislation and College Policies

Legislation

UK General Data Protection Regulation 2018
Data Protection Act 2018
Privacy and Electronic Communication Regulation 2003
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Environmental Information Regulation 2004
Equality Act 2010
Counter-Terrorism and Security Act 2015
Terrorism Act 2006
Computer Misuse Act 1990

Policies

Information Security Policy
Acceptable Use Policy
Home and Remote Access Policy
Account and Password Policy

Glossary

Personal data	Any information relating to a person a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, a ID 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 person.
Special categories of personal data	Types of personal data which is more sensitive and needs more protection. These are: health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, sex life or sexual orientation data.

Processing	In relation to personal data, processing means any operation or set of operations which is performed on personal data (whether or not by automated means). This includes collecting, recording, storing, structuring, altering, retrieving, using, disclosing, publishing and destroying.
Data subject	The identified or identifiable living individual to whom personal data relates.
Data controller	A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Only controllers need to pay the data protection fee.
Data processor	A person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Data Protection Impact Assessment	Data Protection Impact Assessments assess the impact of personal data processing against the rights and freedoms of individuals data is collected about.
The College	The Royal College of Art is the ‘Data Controller’ and is therefore legally responsible for determining the purpose and means of processing personal data in the accomplishment of its missions.