Royal College of Art

Data Protection Policy

Version	2
Date	Aug 2024
Reviewed	No less frequently than every 3 years.
Approved by	Executive Board
Target audience	All staff
Cascaded to	All staff via website
Policy Lead	Alex Smith alex.smith@rca.ac.uk
Owner	Data, Records and Information Officer (DPO)
Department	VCO & Governance

Data Protection Policy

Contents

1. Purpose

The Royal College of Art 'the College' is committed to meeting its statutory and regulatory obligations under the UK Data Protection Act 2018 and UK General Data Protection Regulation (GDPR).

This policy describes how these duties are met and ensures that the College and its staff comply with current 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.

2. Scope

All staff, including temporary agents, contractors and volunteers are responsible for handling personal data in compliance with UK data protection laws on behalf of the College and must adhere to this policy.

This policy applies to all personal data that is processed by the College, including: digital, hard copy, photographs, video, audio and any data that enable the College to identify a data subject.

College Commitments:

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.

3. Accountability and Governance

As the Data Controller, the College understands the importance of Accountability under data protection legislation and puts measures in place to demonstrate compliance with the Accountability principle of GDPR, Article 5(2). It does this by:

- Ensuring all staff complete mandatory Data Protection training;
- Having a robust suite of Data and Information policies in place;
- Maintaining relevant documentation including a Record of Processing Activities, Data Protection Impact Assessments on high risk processing and Privacy Notices;
- Provisions within the College's Financial Regulations for data protection where third parties process personal data on the College's behalf;
- Implementing appropriate and proportionate technical and organisational security measures;
- Implementing a statutory Data Protection Officer;
- Implementing a Data Governance Framework that establishes organisational roles and responsibilities providing accountability for data compliance across the College.

4. Data Protection Principles

Staff are required to adhere to processing personal data following the UK GDPR data protection principles. Principles are always 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.

5. Privacy by Design and Default

The College operates a ‘Privacy by Design and Default’ approach to personal data processing. Ensuring data protection issues are considered as part of design and implementation of our systems, services, products and practices. The data life cycle is considered, including collection, storage, sharing and deletion of personal data.

Collecting personal data

- Before collecting or creating personal data, staff must consider the impact its use could have on the rights and freedoms of the data subjects;
- Personal data being created or collected must be described in a Privacy Notice shared with data subjects;
- If staff intend to conduct systematic and extensive profiling, process special category data on a large scale or systematically monitor a public area they must complete a Data Protection Impact Assessment and have it reviewed by the Data Protection Officer to assess risk and implement risk mitigation strategies.

Securing personal data

- Personal data must be stored on College systems within the College IT network which are maintained and secured by IT;
- Personal data must remain confidential and should not be disclosed to unauthorised third parties;
- Staff must follow Information Security policies and complete mandatory Information Security training;
- Staff must ensure systems and applications containing personal data are administered by default to keep information secure so that personal data has restricted and managed access;
- Requests for personal data disclosures that are not authorised within existing procedures or agreements should be assessed by the Data Protection Officer before disclosure;
- Physical access to buildings or areas where personal data is stored are locked, secure and monitored;
- Staff should avoid processing personal data in public spaces and if such processing is necessary they will ensure the privacy of personal data in these spaces following the Information Security Policies.

Sharing personal data

- Staff should avoid sharing collections of personal data using emails attachments (using workspace or drives links instead),
- When sharing special category data, staff should ensure additional protections are in place (such as password protection or email confidential mode);
- Personal Data used in management reports should be anonymized wherever possible;

- Staff should access and store personal data on centralised single source records wherever possible (such as Thesis, iTrent, and Raiser's Edge);
- Personal data must remain accessible to staff who require it to complete their roles including that staff finance data can be 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 any situations where data protection laws are used to prevent internal access to personal data, the Data Protection Officer will advise best practice.
- Staff members using a third party for personal data processing on the College's behalf must have a Data Processing Agreement in place, following the College Financial Regulations;
- It is recommended that staff setting up a partnership with another organisation that involves sharing or collecting personal data should seek to have a Data Sharing Agreement in place;
- Staff members asked to share personal data with government authorities (such as police or agencies) outside of existing policy or procedures, should seek the advice of the Data Protection Officer.

Deleting personal data

- Personal data will not be held for longer than necessary.
- Personal data is deleted securely with consideration of duplicate data and backups.

International transfers

- Staff must ensure that international transfers of personal data to countries not deemed to have adequate data protection provisions in law have other appropriate safeguards in place;
- Staff must not transfer personal data to countries that are not deemed adequate without these safeguards.

6. Data Subject Rights

All data subjects are entitled to exercise their rights under Data Protection laws and they can be made in writing or verbally. The College will respond to requests within 1 calendar month or in exceptional circumstances this may be extended to 2 months.

Subject Access Requests, or requests made to the College relating to these should be shared with the dpo@rca.ac.uk for handling, unless it is falls within standard operational procedures.

Staff should be aware that Data Subject rights may not apply in all cases and where responsibility of the College is unclear or an exemption may apply, the Data Protection Officer will advise.

The Data Subject Rights are:

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

7. Exemptions

In some circumstances the College may choose to apply data protection exemptions to its processing. Exemptions are never routinely relied on and are always considered on a case-by-case basis. Decisions are documented where exemptions are applied and it ensures that any contingent conditions are met.

This policy does not list all possible exemptions and can be advised on in a case-by-case basis by the Data Protection Officer.

8. Data Breach Incident Procedure

A Data Breach Incident is a breach of security, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- All staff must report personal data breaches to the Data Protection Officer and IT Service Desk using the data breach form (found on the intranet) at the point of discovery, and must provide all known relevant information;
- If information surrounding the breach is not fully known, the incident must still be reported for further investigation;
- All staff must immediately report loss of RCA devices to the IT Service Desk.

Investigation stage

All data breach incidents are recorded by the Data Protection Officer and each incident is investigated and assessed to determine if the breach is likely to result in a risk to the rights and freedoms of the impacted data subjects and whether this risk is high.

Risks include, but are not limited to:

- Discrimination;
- Reputational damage or social disadvantage;
- Financial damage;
- Identity theft/fraud;
- Loss of confidentiality.

The Data Protection Officer will determine whether the risk level is 'high' based on:

- The likelihood of the impact occurring;
- Emotional distress and potential severity;
- Physical damage and potential severity;
- Material damage and potential severity.

Outcomes of investigations, including determining factors causing the breach are recorded with mitigating actions. The record will contain whether the incident has been reported to the Information Commissioner's Office and any outcome of this report.

External reporting

Breaches that result in a risk to the rights and freedoms of individuals are reported to the Information Commissioner's Office by the Data Protection Officer within 72 hours of discovery.

The report will communicate:

- A description of the personal data breach including the type of data, the number of data subjects concerned, the categories and approximate number of records concerned;

- Name and contact details of a contact point;
- A description of the likely consequences of the breach;
- A description of the measures taken or proposed to mitigate adverse effects.

The Data Protection Officer will consider whether it is necessary or appropriate to inform the data subject of the breach. Breaches that are considered 'high risk' will always be communicated to the data subject.

Where appropriate, the College will communicate to the data subject:

- A description of the personal data breach;
- Name and contact details of a contact point;
- A description of any likely consequences of the breach;
- A description of measures proposed or taken, to mitigate adverse effects.

Mitigation

Staff members will work in collaboration to mitigate and manage the effects of data breaches at the College. Mitigating actions will be advised on by the relevant staff members, including the Information Security Manager and IT Services Manager.

Mitigation action may include (but is not limited to):

- Additional staff training;
- Removal of access to systems;
- "Bricking" of RCA devices;
- Deletion of emails within RCA owned inboxes;
- Records management practices such as labelling and file re-structures.

9. Breach of Policy

The Data Protection Officer may recommend further training for staff, or in some cases, the instigation of the relevant disciplinary policy or misconduct procedure where evidence of non-compliance with the Data Protection Policy arises.

10. 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.

Appendices

Royal College of Art

Postgraduate Art and Design

Data Protection Impact Assessment (DPIA)

If you're running a project or programme that involves the use of personal data you may request or require a Data Protection Impact Assessment.
DPIA's are **required** where:

- systematic and extensive profiling of individuals occurs, with significant effects;
- special category or criminal offence data is processed on a large scale;
- systematic monitoring of publicly accessible places occurs.

DPIA's are **recommended** where:

- you want reassurance your project is data protection compliant;
- you want to to define data protection needs;
- you are seeking advice on the mitigation of data protection risks.

For the assessment:

1. Answer the following questions (Step 1 - 9) about your project or programme to the best of your ability.
2. Send the completed questions to dpo@rca.ac.uk. The DPO will be in touch regarding personal data compliance of your project.

Step 1: Identify need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal.

Step 2: The nature of the processing

1. How will you collect, use, store and delete data?	
2. What is the source of the data?	
3. Will you be sharing data with anyone?	
4. What types of processing identified as likely high risk are involved?	

Step 3: The scope

5. What personal data will you be using?	
6. Will you be using special category or criminal offence data?	
7. How much data will be collected?	
8. How often will the data be collected?	
9. How long will data be kept for?	

Step 4: The context

10. What is your relationship with the individuals?	

11. How much control do they have over the processing?	
0. Do the individuals include children or vulnerable groups?	
0. Are there prior concerns or security flaws? Is the processing novel?	

Step 5: Describe the purpose

0. What do you want to achieve?	
0. What is the intended effect on individuals?	

Step 6: Consultation process

0. Have you consulted anyone? (internal or external) Or do you intend to consult anyone?	

Step 7: Necessity and proportionality

0. Is there another way to achieve the same outcome?	
0. How will you prevent function creep? Or onward use of the data?	
0. Have you got a Privacy Notice? Or is your processing part of an existing Privacy Notice?	

0. Has the DPO reviewed any partnership contracts?	

Step 8: Identify and assess risk

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 9: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8				
Risk	**Options to reduce risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 10: Sign off and record of outcomes

Item	Name/position/dates	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 9 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses review by:		If your decision departs from individuals 'views', you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

[Template] Privacy Notice

Last updated: XXXX

Types of personal information we process

[DESCRIBE OR LIST THE CATEGORIES OF PERSONAL INFORMATION YOU ARE USING]

Why we process your personal information

[DESCRIBE OR LIST EACH OF THE PURPOSES THAT YOU ARE COLLECTING USING THE DATA FOR. EG. 'To process your application', 'to provide you with x service'.

Our lawful basis

[ADD THE RELEVANT DATA PROTECTION LAWFUL BASIS FOR YOUR PURPOSES, SELECT ALL THAT MAY APPLY]

- Necessary for our public task, Article 5 [EG TO PROVISION EDUCATION]
- Legitimate interests, Article 5 [EG. TO PROVIDE SECURITY]
- Legal obligation, Article 5c [EG. OFS/GOVERNEMENT REQUIRED]

- For the performance of a contract, Article 5 [EG. TO FULFIL A CONTRACT WITH THE DATA SUBJECT]
- Vital interests, Article 5 [EG. TO PROTECT SOMEONES LIFE]
- Consent, Article 5 [WITH THE DATA SUBJECTS CONSENT]

How we may share your personal information

[DESCRIBE OR LIST THE ORGANISATIONS OR CATEGORIES OF ORGANISATIONS THE PERSONAL DATA WILL BE SHARED WITH]

[EG RCA FINANCIAL SERVICE PROVIDERS]

How your personal information is stored

[DESCRIBE THE SECURITY PRACTICES RELEVANT FOR YOUR PROCESSING]

[EG. We operate secure electronic and physical storage with controls for personal data. We employ robust technical measures such as encryption when storing and transmitting your personal data. RCA staff are subject to mandatory data protection and information security training.]

Your rights

When the College processes your persona data, you have the following qualified rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making
-

To make a request under any of these rights, or to contact us about your personal data please email dpo@rca.ac.uk. Or by writing to:

Governance team
Royal College of Art
Kensington Gore
London SW7 2EU

If you would like to make a request by phone please call us at +44 (0) 207 590 4444 and leave a message.

You also have the right to make a complaint to the Information Commissioner's Office at www.ico.org.uk. Or by writing to:
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Data Security Breach Form

This can be accessed via the intranet and ServiceNow and includes the following questions.

Report Data Security Breach

Form to report perceived or potential a breach in data security

This form allows all staff to report breaches in RCAs data, whether malicious in nature or accidental

Summary

1. A description of the breach and any corrective actions taken at the time of discovery. Please provide as much information about the breach as possible.

2. When was the breach discovered?

3. When did the breach take place?

4. Is special category data involved? (e.g. Racial or ethnic origin. Political opinions or religious or philosophical beliefs. Membership of a trade union. Physical or mental health or condition or sexual life.

5. Is special category data involved? (e.g. Racial or ethnic origin. Political opinions or religious or philosophical beliefs. Membership of a trade union. Physical or mental health or condition or sexual life.

6. Where did the breach take place?

7. Type of breach?

8. Who is the affected individual?

9. Estimated number of individuals affected?