Royal College of Art

Information Handling 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

Information Handling Policy

Contents

1. Purpose and Scope

This policy describes how all staff (including contractors, volunteers and agents) should manage the College's information and data. It sits within the Data and Information Policies to provide everyone who works for the college with clear and consistent instructions on how to protect themselves, others, and college assets.

The policies and associated processes are designed to reduce information-related risk to tolerable levels. All users must adhere to these policies to enable the college to run effectively and to keep the college and its people secure from information risks, such as ever-evolving cyber threats or non-compliance with the Data Protection Act 2018.

The policy refers to and outlines the management of information assets. Information and data assets can take physical and digital forms, including paper files, documents,

databases, and video or audio recordings. Everyone must take adequate steps to prevent accidental or deliberate disclosure and unauthorised access to these assets.

Definitions

Information Assets are defined as a group of information that can be defined and managed as a single unit so that it can be understood, shared, protected, and exploited efficiently.

Example: a student record, mailing list, or documentation relating to a specific project are examples of Information Assets.

Data are defined as information constituting facts or figures used to analyse something or make decisions.

Information is the organisation or interpretation of data to give meaning within a context.

Records are defined as information consciously retained as evidence of an action.

Retention refers to the ability to store and recall data, information and records, and the period for which the College will no longer require it.

2. Responsibilities

All staff

All Staff members employed by the College are responsible for handling the College's information and data in line with this policy to keep information secure, ensure statutory and regulatory compliance, and support the efficient running of the College. The full set of Information Security and Data policies are listed at the end of this Policy.

Managers

Managers must ensure staff are aware of and comply with information policies, complete mandatory training (including any additional training required for certain roles), and report non-compliance.

Data Owners

Schools and Professional Services must have one named individual to take accountability for information and data assets as the Data Owner. The Data Owner will be responsible for ensuring data managed by their team, service, or School is processed (e.g. used, stored, shared, and destroyed) in compliance with the Data Protection Act 2018, including maintaining data integrity and quality, maintaining retention periods, and keeping confidential information assets secure.

Data Stewards

Data Owners will nominate at least one Data Steward for their area of the College to support the effective management of information and data. The Data Steward will do this through the implementation or development of compliant procedures, identifying risks to the Data Owner, and communicating data and information practices to their teams.

Senior Information Risk Owner

The College has a nominated Senior Information Risk Owner who owns the College's data policies and is accountable for data risk decisions. The role reports information risk to the Executive Board and Council, and leads on and fosters a culture that values data and best practice data governance.

The College

The College is responsible for compliance with legal and statutory duties related to this policy.

3. Classifications

Data Owners must periodically audit and assess the risk to information assets to determine the sensitivity to apply appropriate security measures and information handling procedures.

The use of classification labels against documents is encouraged to convey the confidential nature of a document. The level of protection required is proportional to its classification (more sensitive data requires additional security measures). The College defines its information assets as one of the following classification types:

Public Information (Unrestricted)

Information is available to anyone (including members of the public). Such information should be stored on College systems where possible to maintain availability and appropriate management of data.

Impact of Disclosure: Little to no damage.

Restricted information

Information that is not routinely made available to the public and does not attract confidentiality requirements internally. Can constitute internal procedural documents, general reporting data, CAD designs, and materials under copyright.

Impact of disclosure: Low reputational or financial impact where inaccurate information is disclosed inappropriately.

Confidential information

Access is restricted and limited to an authorised group internally. Information in this class may include but is not limited to:

- commercially or financially valuable information;
- student coursework and exam scripts;
- internal reports;
- general research data held;
- Protected Personal Information (information that links an identifiable individual with information that, if released, would put them at significant risk of harm or distress);
- any source of information relating to a substantial number of individuals.

Impact of disclosure: Moderate to significant reputational damage, financial damage, and damage to individuals through non-compliance with statutory and regulatory duties.

Strictly Confidential information

Access is restricted to a small, named group, regularly reviewed, and requires additional protection. Information in this class may include but is not limited to:

- Special category data, as defined by UK GDPR;
- Research data covered explicitly by a patent or legal agreement;
- Information protected by clauses;
- Evidence of criminal activity;
- Reports under the Whistleblowing procedure;

- Highly sensitive financial information.

Impact of disclosure: Significant to substantial reputational damage, financial damage, and damage to individuals through non-compliance with statutory and regulatory duties.

4. Information and Data Management

All staff are responsible for handling information assets and should consider all stages of the data life cycle from creation to disposal when applying measures to keep information secure, accessible, compliant, and of good quality.

Individual information assets or processes relating to information assets should be regularly reviewed to ensure data compliance and security.

Plan & Design

- The College takes a 'Privacy by Design' approach to personal information privacy and confidential information. Systems should be designed as default to private with access actively enabled for appropriate groups or individuals.
- The College seeks to maintain data accuracy by using single source data records (aka 'master record', 'golden source' such as Thesis, Unit4, and iTrent). Staff should consider whether the data already exists before trying to recreate or duplicate data.

Collect or Create

- Label or name your information clearly so that it can be understood by other staff members. Staff are encouraged to use 'confidential' and 'strictly confidential' labels to alert colleagues that information requires secure handling.
- Consider the source of your data, and whether it requires validation for accuracy.
- Inform individuals about what you're doing with their personal data, including if you are using automated transcribing or notetaking services that collect their data (image or audio recordings, or personal opinions).
- Consider how your methods of data collection can support the data quality principles of completeness, uniqueness, consistency, timeliness, validity, and accuracy.

Storage

- Do not keep information on local computer drives (e.g. ‘C drive’ or local ‘My Documents folder). Use college-approved storage such as Google drive or the network file share.
- Wherever possible, do not store college data on the Google My Drive and opt for a Shared Drive. Managers should follow the Leaver’s Checklist procedure to ensure that information is handed over at the end of employment.
- Keep confidential paper records secure (e.g. a locked cabinet).
- Do not use a USB drive as a permanent storage solution. They should only be used to store non-confidential data for short periods.

Use & Share

- Confidential and Strictly Confidential information should only be shared with authorised individuals. Where authorisation is not clear the staff member should seek guidance from their local Data Steward or Data Owner.
- Consider the sharing method as not all systems are considered secure (e.g. Sending confidential information by email can be intercepted, and easily sent to the wrong person).
- Consider the type and volume of data and the impact of improper disclosure.
- Confidential information must be protected (e.g. encrypted) when sent outside of the organisation or transferred to external media (e.g. memory stick).
- Organisations that work with the College on shared data will need to have sufficient technical and organisational security guarantees.

Retention - Disposal or Archive

- Data and Information must be held in line with the college’s Retention Schedule, and personal data must not be held for longer than necessary under business or legal requirements.
- The Data Owner is responsible for ensuring that their School or Team information is maintained following the retention schedule, or as in line with business requirements providing that regulatory or statutory requirements are met.
- In some cases files will be held permanently for contractual or legal reasons, or information of special interest may be archived. Staff will need to consider how to store permanent materials securely and sustainably so that it remains accessible to the College. Special-collections@rca.ac.uk can be contacted for guidance on archiving records.
- Records should be destroyed or deleted securely with consideration for duplicate data and backups.
- Confidential paper materials should be destroyed using confidential waste bins.

5. Compliance

The College and it's staff must comply with legislation, the following legislation are most relevant to this policy:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- UK General Data Protection Regulation (GDPR) 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Terrorism Act 2006
- Privacy and Electronic Communication Regulations 2003
- Counter-Terrorism and Security Act 2015.
- Limitations Act 1980.

6. Policy Review

This policy will be reviewed as it is deemed appropriate, but no less frequently every three years.

7. Related Policies

Information Security Policy

Account and Password Policy

Acceptable Use Policy

Information Handling Policy

Home and Remote Access to Services Policy

Data Protection Policy

Data security breach process