Royal College of Art Postgraduate Art & Design	**Royal College of Art** **Data Governance Framework**

Version	2
Date	March 2024
Reviewed	No less frequently than every 3 years.
Approved by	SMT
Target audience	SMT
Available to	All staff
Policy lead	Alex Smith alex.smith@rca.ac.uk
Owner	Data Protection, Records and Information Officer
Department	VCO & Governance

Contents

1. Introduction

Data and information are vital and valuable resources. The availability of high quality data and information enables the Royal College of Art ("The College") to carry out its function as a higher education and research institution. It is therefore imperative that the College

manages its data and information assets with care so that they can be used to enable good decision making, enhance service operations and meet statutory obligations.

The following Data Governance Framework ("the Framework") sets out the College's commitment by bringing together a network of people, policies, procedures and controls which establish good data governance across the College. The Framework underpins the structural and operational management of data to ensure its security, quality and integrity in meeting its institutional objectives and legislative, regulatory, and contractual requirements.

2. Scope & Definitions

2.1 The Framework is relevant to anyone working at the College. This includes all staff, temporary, casual, contract, agency staff, and service providers acting on behalf of the College.

2.2. Staff must be familiar with the Framework and have a responsibility for implementing and embedding relevant aspects of the Framework into their working practices.

2.3. The Framework applies to all data and information assets, encompassing data stored in digital networks and drives, paper records, communications, video/audio recordings and photographic media whether created, received or maintained in the course of carrying out College business.

2.4 The Framework applies to all information and data at the College. For simplicity, the Framework refers to both information and data as 'data'. A further glossary of terms can be found in Appendix 1.

3. Data Governance Framework

3.1 Strategic Objectives

The Framework sets out the following strategic objectives:

- Drive a coherent and comprehensive approach to data asset management as a key institutional asset;
- Maintain high quality data to support strategic objectives and decision making at a senior level;
- Demonstrate accountability to public, private regulators and sponsors;
- Report maturity and risk assurance relating to records management activities;
- To promote a data governance culture which recognises data as a key asset;
- Identify key roles and responsibilities within data governance to support effective practice of the management of information across all business areas.

3.2 Data Governance Network

3.2.1 The Data Governance Network outlines roles and responsibilities for data governance across the College to embed accountability of data and provide a support framework for best practice and decision making.

3.2.2 The Senior Information Risk Owner is accountable for information risks and the implementation of the Data Governance Framework on behalf of the College. Implementation is supported by the Data Governance Working Group.

3.2.3 The Data Governance Working Group provides expert guidance, strategic direction, policy review and risk monitoring for data at the College. It also acts as a rapid response group convening on cases of serious data incidents and is responsible for managing the containment, mitigation, and communication of data incidents.

3.2.4 Roles of the Data Governance Network are outlined below:

Scope	Title	Role
College	Senior Information Risk Owner (SIRO)	Owns the College's data risk policies and data governance framework. Reports to CEG/Council on data risk decisions. Leads on and fosters a culture that values data and best practice data governance.
	Chief Information Officer and Director of Digital Delivery and Technical Services (CIO)	Establishes and maintains strategy and programme to secure technology and systems.
	Data Protection Officer (DPO)	Works across the network to advise the College of its obligations under data protection law. Monitors data protection compliance and conducts compliance risk assessments. Acts as point of contact for all data subjects and the ICO on data protection matters.
	Data Asset Owner	Accountable for compliant data processes in their key area; determines how and why data is used. Manages data risks and where necessary reports them to DPO or

Department		SIRO.
	Data Asset Steward	Supports the Data Asset Owner in managing compliant data processes. Acts as key departmental contact for department data compliance queries and disseminates communications and best practice in their department. Reports data risks to DPO or Data Asset Owner.
	Data Asset Administrator	Provides administrative support to the Data Asset Manager in maintaining quality of data assets and fulfilling data requests. Reports data risks to the Data Asset Manager.
Individual	Principal Investigator	Only applies to Research. Specific to research project data, roles are equivalent to the Data Asset Owner at minimum. Data Asset Manager and Data Asset Administrative roles may be applicable to projects.
	Staff	All staff are responsible for familiarising themselves with the College's information policies and following the data management principles. Staff are responsible for reporting personal data breaches.

3.3 Data and Information Handling

3.3.2 The Data and Information Handling Policy sets out the methods by which all staff at the College, except those undertaking research, should manage data at the College. The Research Data Management Policy sets out the methods by which Research staff should manage Research data. Staff should familiarise themselves with the relevant policy and embed the practices into their work.

3.3.3 The DPO and Data Asset Owners will maintain an Information Asset Register with Records of Processing Activity on behalf of the College. This documentation provides assurance to the College through oversight of data assets, ensuring compliance with GDPR and relevant legislations.

3.3.4 The College processes information in compliance with key information legislation: General Data Protection Regulation 2018, Data Protection Act 2018, Freedom of Information Act 2000, Environmental Information Regulation 2004 and Privacy and Electronic Communications Regulations 2003. The College publicises methods to access

information under these legislations and supports transparency and openness through its policies and procedures.

3.4 Policies and Procedures

3.4.1 Members of the Data Governance Working Group review and recommend changes to, or new data governance policies. Policies are made available to staff on the College's website.

3.4.2 All policies are reviewed no less frequently than every 3 years.

3.4.3 Data Governance Framework encompasses the following Policies and Procedures:

Policy/Procedure	Owner	Status
Acceptable Use Policy	ILTS	Published
Account and Password Policy	ILTS	Published
Data Protection Policy	Governance	Published
Home and Remote Access Policy	ILTS	Published
Information Security Policy	ILTS	Published
Data and Information Handling Policy	Governance	Published
Freedom of Information Act Policy	Governance	Published
Freedom of Information Act Procedure	Governance	Published
DPIA Procedure	Governance	Published
Data Breach Procedure	Governance	Published
CCTV Policy	Estates/Governance	Published
Research Data Management Policy	Research	Published
Data Retention Policy	Governance	Not yet published
Personal Device Policy	ITLS	Not yet published

3.5 Risk Management

3.5.1 Risks to data are recorded by Data Asset Owners within operational risk registers. Large scale and priority risks are escalated to Senior Information Risk Owner and brought to the Audit & Risk Committee via the strategic risk register.

3.5.2 Continuous monitoring of personal data incidents and breaches is conducted by the DPO through a maintained breach report that supports operational risk monitoring.The DPO will communicate reportable breaches to the Information Commissioner's Office within 72 hours of discovery.

3.5.3 The Data Governance Working Group meets to respond to serious data incidents. The group defines and executes a response plan to mitigate risk and secure data. Members will invite relevant key Data Asset Owners.

3.5.4 Digital information security monitoring is managed by Technology. All staff must complete the Information Security training and comply with policy and technical controls to access data held by the College. The College responds to Cyber incidents via the Cyber Incident Response Plan.

3.5.6 The Council is responsible for appointing auditors for the assessment of data risk, following the Internal Audit Policy and Procedure.

3.6 Quality Monitoring

3.6.1 The College conducts annual data quality audits across student, staff and financial data which ensure quality of College master record data. Data quality checks are completed for business functions in supporting the Colleges' strategic objectives and to meet statutory and regulatory external reporting requirements.

3.6.2 The College is obligated under statutory and regulatory duties to submit annual external data reports to the OfS including HESA Student Return, HESA Staff Return and the Annual Financial Return. The Annual Financial Return must be consistent with the College's latest audited financial statements. The College submits non-annual external data reporting via the Research Excellence Framework.

3.6.3 Data Asset Owners are responsible for timely submission to meet these duties. The reporting is overseen by the Senior Information Risk Owner under the Data and Compliance Audit Schedule.

3.6.4 Data Asset Owners are responsible for implementing data processing procedures that incorporate data quality control measures. These measures ensure data quality is

maintained throughout its lifecycle and distribution within the College as relevant to its use.

3.7 Access Controls

3.7.1 Where personal or confidential data is stored on College systems, access permissions are set at user level to protect the data and information from inappropriate access and to limit availability to required users only.

3.7.2 Access permissions are granted via Data Asset Owners or responsible Data Stewards of the relevant data within the College system, and permissions are equipped by IT system administrators.

3.7.3 Data Asset Owners are responsible for documenting and publishing access control procedures for the College's core master record systems for student, finance, staff, alumni and research data.

3.7.4 Data Asset Owners are responsible for ensuring system users have completed applicable training before College system access permission is granted, including completion of GDPR training for access to personal data.

3.7.5 Data Asset Owners are responsible for, at minimum, an annual review of College system access control permission lists where systems are set by user-based role to ensure access is appropriate.

3.7.6 All staff must follow the Information Security policies when accessing the College's network.

3.8 Training

3.8.1 Data Governance training and development is essential for the development of staff knowledge and skills relating to information management, data protection and information security across the College.

3.8.2 GDPR and Information Security training are mandatory requirements for all new staff as part of their induction. Training can be accessed via Moodle and staff should aim to undertake the training every 3 years to refresh their knowledge.

3.8.3 All staff should familiarise themselves with the Information and Data Policies and procedures relevant to their work.

4. Appendices

Appendix A – Glossary of terms

Data	Data is individual facts and figures.
Data Set	A Data set is a collection or tabulation of data.
Information	Information is the organisation and interpretation of data to make it meaningful in a context.
Personal data	Information relating to an identified or identifiable natural person; 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 person.
Special category data	Identifiable personal data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, data concerning a person's sex life, and data concerning a person's sexual orientation.
Asset	A body of information or data defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently.
Information Asset Register	A list of key data and information assets owned by the College.

Record of Processing Activity	As specified by GDPR, a list of personal data assets and related information: lawful basis, retention, security, data categories, automated processing and international transfers.
Master Data Record	The College's core data sets: Student Registry, Staff Registry, Financial System, Research System and Alumni Registry.
Senior Information Risk Owner (SIRO)	Owns the College's data risk policies and data governance framework. Reports to CEG/Council on data risk decisions. Leads on and fosters a culture that values data and best practice data governance.
Data Asset Owner	Accountable for compliant data processes in their key area; determines how and why data is used. Manages data risks and where necessary reports them to DPO or SIRO.
Data Asset Steward	Supports the Data Asset Owner in managing compliant data processes. Acts as key departmental contact for department data compliance queries and disseminates communications and best practice in their department. Reports data risks to DPO or Data Asset Owner.
Data Asset Administrator	Provides administrative support to the Data Asset Manager in maintaining quality of data assets and fulfilling data requests. Reports data risks to the Data Asset Manager.

Appendix b – Tools

Retention schedule