Royal College of Art

Information Security: Information Security Policy

Revision History

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

Version	Status	Owner	Reason for change	Date	Next Review Date
0.3	Draft	IT	document creation	Aug 2021	
1.1	Approved	IT	review / peer review	Jun 2022	
1.1	Sign off	IT	SMT sign off	Aug 2022	Aug 2024
2.0	Draft	Technology	review	July 2024	
2.0	Sign off	Technology	Executive board signoff	Oct 2024	Oct 2026

Table of Contents

Contents 2

Purpose and scope 3

Information security fundamentals 3

- Responsibilities 4
- Monitoring 5
- Audit Logging 5
- Asset Management 6
- Access control 6
- Supplier relationships 7
- Information security incident management 7

Compliance 7

Data security breaches 8

Third-party services 8

- Google 9

Training and awareness 9

- Information security training and guidance 9

Policy Review 9

Related policies 10

Related Processes 10

1. Introduction

The Information Security and Data policies provide everyone (staff, students, third parties, contractors, consultants etc.) with clear and consistent instructions on how to protect themselves, others and College Technology assets (e.g. data and services). The policies, associated processes and procedures are designed to reduce information-related risk to tolerable levels.

The College is committed to compliance with GDPR and UK Data Protection Act 2018 and to ensure that the College's Data Privacy and Information security policies are being followed.

2. Purpose and scope

This document overarches all Information Security policies. It sets out the high-level expectations for anyone processing information (digital or physical) on behalf of the College.

This policy applies to all students, staff including partners, contractors, consultants and third parties working on behalf of the college. All must adhere to this policy to keep the College and its people secure from Information security risks.

Non-compliance of policies puts people and the College at risk. A breach of information security presents a risk of cyber threats which may result in damage to you, our students, your colleagues, or the College through the loss of control over personal data or confidential data, identity theft, fraud, financial loss or reputational damages.

Therefore, non-compliance may lead to the removal or disablement of Technology equipment, services and accounts. In some cases, disciplinary measures might be pursued, which may also lead to legal action.

3. Information security fundamentals

Information and systems must remain secure and private. Whilst the information security team will be mindful of the approaches adopted by its stakeholders, everyone must agree to and uphold the following information security fundamentals:

1. Consider and process information (e.g. confidential student record or restricted commercial document) according to the *''Information Handling Policy''*;
2. Safeguard information (according to its classification) with appropriate security measures (e.g. encryption) to protect against unauthorised access;
3. Make information available only to those who have a legitimate right or

authorisation to access it;
4. Report breaches of the information security policies to Technology;
5. Take personal responsibility for Technology resources (e.g. computers, accounts, storage) and use in line with the policies.

3.1 Roles and Responsibilities

Individual responsibility for information security within RCA is as follows:

- **The Chief Operating Officer** acts as Senior Information Risk Owner, taking accountability for information risk;
- **All staff :** using College services has a responsibility to protect data and systems in their control. Those responsibilities are defined in the Information and Data policies.
- **Managers :** must ensure staff are aware of and comply with information security policies, complete mandatory training (including any additional training required for certain roles e.g. Finance), report non-compliance and maintain the confidentiality, integrity and availability of College information assets.
- **Information Security Manager :** is responsible for the delivery of a suitable and robust information security programme that identifies and addresses security and privacy risks.

Where practical, security responsibilities will also be included in role descriptions and personal development plans.

4. Controls

RCA adopts a risk based approach to the application of Information Security control measures (4.1-4.10)

4.1 Information security policies

There are enterprise level information security policies that are signed off by the Executive board which are published and communicated on the RCA website and intranet.

There are a set of lower level controls, processes and procedures for information security, defined in support of the high level Information Security Policies. This suite of supporting documentation will be approved by the Head of IT, published and communicated via the

intranet.

4.2 Monitoring

Technology does not routinely monitor internet usage, electronic communication (e.g. email), documents (e.g. on Google Drive) or other digital information.

Such information may be accessed where necessary to protect the rights, property, or personal safety and to preserve the integrity of systems (e.g. investigations as a result of a security breach) of the College, students and staff, or to comply with legal obligations, such as responding to requests from enforcement agencies, requests for personal data from individuals, court orders, or other legal processes.

Monitoring and access is conducted by System-level and privilege staff users for reasons set out above. System-level staff account access is managed following the Account and Password Policy.

4.3 Audit Logging

Most College systems maintain transactions and events, this is required for operational management and security. The College is mandated to ensure regulatory requirements for safeguarding the confidentiality, integrity, and availability of information assets through auditing, logging, and monitoring activities . This may include but not limited to the logs for:

- The geographic area where a device is using College websites, applications or services;
- Normal system events – such as start-up, shutdown, login attempts, errors, security policy changes, software installations;
- Device data such as type of software and hardware used, IP address, browser type and settings, date and times (e.g. creation, modification and erasure), language preferences, and cookie information;
- Unauthorised access to confidential data for non-permitted purposes;
- System management activities – including execution of privileged functions;
- Information exchanges containing confidential data;
- Activities relating to administration account(s).

4.4 Asset Management

All assets documented and accounted for to include:

- software;
- information processing hardware such as laptops, desktops etc

Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

All information assets are managed through the Data Governance Network structure and have an accountable Data Owner to ensure appropriate handling.

The RCA operates a one laptop policy, staff are responsible for the laptop they have been assigned and must return an old device if upgrading to a new one. All allocated laptops remain the property of RCA and must be made available when requested.

4.5 Access control

The College operates on the principle of least privilege, and therefore only the appropriate level of access will be provided based on the business requirements. Mandatory two factor authentication methods are in place.

The HR formal starter and leaver process will be used to maintain access to all information systems and services to ensure that access to systems are timely revoked or granted.

Specific controls will be implemented for users with elevated privileges to ensure the separation of duties and to reduce the risk of negligent or deliberate misuse.

4.6 Change management

A change is a modification to an application live environment, such as a change of functionality or a change in user experience . Change management plays an important role in ensuring that only authorised changes that have been documented and have gone through the change process are deployed.

Changes should be deployed in a manner that does not have an impact on infrastructure and day to day activities of staff and students.

4.7 Supplier relationships

RCA's information security requirements must be considered when procuring or establishing relationships with suppliers to ensure that information assets accessible to

suppliers are protected.

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

4.8 Vulnerability & patching management

All Technology systems must be supported and have up to date security patched operating systems and application software. In the event of unsupported legacy systems, these should be moved to another system and decommissioned. If decommissioning is not possible then the system must be segregated to mitigate risk to the corporate network.

Where the responsibility of patching falls on the vendor/supplier, service level agreements must be in place that address updating in a timely manner.

The information security function provides advice on security risks and the appropriate mitigating measures. They are responsible for running network vulnerability scans ,distributing the results, tracking actions and escalating issues via the Technology reporting line wherever needed.

4.9 Security operations

The information security function will ensure the correct and secure operations of information processing to include:

- documented standard operating procedures for information security;
- formal change and capacity management for information security;
- controls against malware;
- identity and access management;
- vulnerability management.

4.10 Information security incident management

Staff are requested to report any suspicious emails or activity to the service desk so actual or suspected information security breaches can be investigated and appropriate action taken to mitigate the breach.

5. Compliance

The College, each student and member of staff have an obligation to abide by all statutory, regulatory and contractual security requirements.

Compliance with the controls in this policy will be monitored by the information security function.

6. Data security breaches

The College must inform relevant legal and regulatory entities when certain data security incidents occur. For example, where there is a reportable personal data breach, the College must inform the Information Commissioner's Office within 72 hours. It is, therefore, essential you report data security breaches via the Data Breach Form immediately to limit the impact to the College and individuals.

Some examples of data security incidents are:

- Loss or theft of confidential information (e.g. documents taken from a car or left in a cafe);
- Loss or theft of equipment used to store confidential information (e.g. laptop, smartphone, USB stick);
- Accidental or unauthorised disclosure of 'confidential' or 'strictly confidential' information (e.g. documents sent to an incorrect recipient or incorrect permissions to files);
- Unauthorised access to, removal/copying or modification of records or data;
- A computer system or equipment compromise (e.g. malware, denial of service attack);
- A compromised account (e.g. spoofing, hacking, shared password);
- A compromised location holding confidential information or critical equipment such as servers.

7. Third-party services

Individuals must only use systems provided by Technology Services for carrying out College business. In some circumstances, existing solutions may not meet requirements and therefore using third party services may be possible, but only with the express permission from Technology.

Google

The College uses Google services for the use of email, storing and sharing files in the cloud. Information uploaded to, read, modified and shared using these apps (e.g. Google Mail and Google Docs) are automatically encrypted to ensure the data is secure. Google undergoes

regular independent audits on their data centres (e.g. cloud services), network, and operations (e.g. internal processes). Compliance is certified compliance through industry standards such as ISO 27001 and 27017.

Google processes RCA data in a way that is compliant with both the GDPR and the DPA(2018).

Personal information collected in the Core Services (e.g. Google Mail and Google Docs) is used only to provide the Core Services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.
For more information, please read Google's 'Google Workspace for Education Privacy Notice': https://workspace.google.com/terms/education_privacy.html

8. Training and awareness

The College will provide the necessary resources to help everyone meet their information security and privacy obligations. All staff must complete mandatory training, others may need to complete additional modules depending on their department or school and the confidentiality of the data they manage.

Also part of the awareness training is phishing simulation exercises that will occur at a minimum once every two months. These simulations are designed to reinforce good security practices.

The mandatory awareness course will be audited and reported on a regular basis to ensure compliance.

9. Policy Review

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

10. Related policies and processes

This policy should be read alongside the following 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 (internal)

11. Information security training and guidance

- Information security training (mandatory)
- GDPR training (mandatory)
- Data Security Toolkit