Royal College of Art

Information Security Acceptable Use 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

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

The purpose of this policy is not to impose restrictions but to outline the acceptable use of computer resources owned or managed by the College, with the sole aim of protecting the College, its staff, students and partners confidentiality, integrity, availability, accountability and assurance of RCA's systems and data processing.

Inappropriate use of systems could lead to a cybersecurity breach which may result in damages through the loss of control over personal data or confidential data, identity theft, fraud or financial loss. Policy breaches also put the College at risk of cyber-threats, legal action and regulatory penalties.

The policy applies to all systems and devices used for business purposes including but not limited to intranet/internet, laptops, workstations, mobile devices, software, operating systems, storage media, network connections (wired/ wireless), assigned user accounts and electronic mail.

It 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.

3. Acceptable use policy

Effective security is a team effort involving the participation of every College employee, student and third-party. It is the responsibility of users to know these guidelines, comply with all applicable laws, regulations and policies and to conduct their activities

accordingly.

4. Accounts and passwords

- Individuals given access to College Technology services will be issued a unique ID which may include an email address. It is their responsibility to use strong passwords and take reasonable steps to protect both the ID login and passwords.
- Use different passwords for different sites. Avoid reusing passwords.
- Staff members should not use personal email addresses for work purposes. Personal email addresses are not to be used for work purposes.

5. Technology equipment

Each staff member is limited to one laptop device, if there is a need for a replacement then the older version device must be returned when receiving the newer device.
Technology equipment provided remains the property of the College and is managed by Technology. Individuals must ensure:

- All company assets are returned at the end of their engagement with RCA;
- Fixed items (e.g. monitors, personal computers, printers) remain on-site and connected to the network. Where adjustments need to be made, and computing equipment needs to be taken off-site, permission must be sought from Technology;
- Software is updated regularly *(in some circumstances users intervention will be required to initiate software updates);*
- Devices must be screen-locked when left unattended for short periods and locked away at the end of the day;
- Ensure appropriate care is taken when using computing equipment to avoid damage, loss or theft of items;
- Damage to, lost or stolen items are reported to the Technology Service Desk immediately;
- Equipment is made available to Technology when requested;
- Individuals must comply with any request made to them by Technology staff in connection with the enforcement of this policy.

6. Personally owned devices

Staff are not generally required to use their privately-owned equipment for work purposes; however, in some circumstances, it might be warranted. Responsibility lies with the individual to ensure that appropriate controls are in place to mitigate the increased risk of using their own devices, especially when working with confidential data. This means the

device must :

- Be enabled with disk encryption and protected with a strong password;
- Have a supported operating system with security updates regularly installed, including third-party applications (e.g. Adobe Acrobat);
- Enable auto-lock after a short period (e.g. 10 minutes);
- Have anti-virus software installed, updated regularly and a firewall running at all times;
- Have a separate, secured account for work purposes, so others do not have access to confidential or sensitive information, and ensure the password for the login account is sufficiently long and complex;
- Must not store RCA information on personal cloud storage (e.g dropbox). Only RCA approved cloud storages should be used.

Visit the College's information security intranet pages for help keeping devices up to date and secure.

7. Personal use of College Technology services

Occasional personal use of College Technology services is allowed with the following conditions:

- Such activity must not:
    - interfere with the work of the individual or others;
    - contravene College policies;
    - be excessive in the use of resources.
    - bring disrepute to the College
- Do not store personal files (e.g. photographs, music, correspondence) on College drives (e.g. Google Drive, file shares, disk drives);
- Staff must not use private email addresses to conduct College work.
- Staff are aware that Technology staff may be required to access the Staff member's account and therefore information will be accessible to the RCA.

8. Unacceptable use

The list below is not exhaustive and is an attempt to provide a framework for activities that fall within unacceptable use of the College's Technology systems, services and equipment;

General:

- Carrying out activities that contravenes Jisc (the College's internet service provider) policies (https://community.jisc.ac.uk/library/janet-policies);

- Engaging in illegal and fraudulent activity;
- Providing unauthorised individuals access to College services;
- Carrying out any irresponsible or reckless handling of College data (see the Information Handling Policy);
- Using Technology facilities to cause alarm or distress to others;
- Send unsolicited and unauthorised bulk email (spam) not related to legitimate College business;
- Use College Technology resources to carry out cyber-attacks or break into (hack) College or external computer systems;
- Intentionally deploy any form of malicious software such as spyware, malware, ransomware;
- Create, store, transmit or share material which:
    - is defamatory or obscene;
    - infringes copyright;
    - promotes terrorism or violent extremism;
    - seeks to radicalise individuals to such causes.
- Make configuration changes to the Technology systems that may undermine the confidentiality, integrity or availability of services (e.g. disable antivirus or firewall);
- Circumventing user authentication or security controls;
- Install and use unsupported or unlicensed services without seeking permission from Technology Services;
- Failure to comply with policies and instructions from Technology Services or other authorised staff;
- Failure to report data security breaches to Technology or the Data Protection Officer.

Social Media and Communications:
When engaging on social media, individuals should ensure that they follow the College's social media policy, which can be found here.

9. Exceptions

Any exception to the policy must be approved by the Technology Service Desk. All policy statements must be followed if approved.

Obscene material
In very few circumstances, some individuals are required to view obscene materials (e.g. for academic research or investigative purposes). In these cases, they must seek written approval from an Ethics Committee, or the Chief Operating Officer and inform Technology.

Non compliance

Non-compliances may lead to the removal of Technology equipment, services and account privileges. In some cases, disciplinary measures might be pursued, which may also lead to legal action.

10. Policy Review

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

11. Related policies and processes

- Information Security Policy,
- Account and Password Policy,
- Personal Device Policy,
- Information Handling Policy,
- Home and Remote Access to Services Policy,
- Data Protection Policy,
- Data security breach process (internal).