Royal College of Art

Information Security
Home and Remote Access to Services 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

Using College Technology services remotely (e.g. away from campus) helps us be more flexible and productive. However, it increases the risk to systems and data from unauthorised access. This policy defines the requirements for connecting to Technology services remotely and sets out the responsibilities for everyone who uses College resources externally, helping them reduce and mitigate these risks.

This policy applies to all students and staff including partners, contractors, consultants and third parties working on behalf of the college. Everyone 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. Therefore, non-compliances may lead to the removal or disablement of Technology equipment, services and accounts. In some cases, disciplinary measures might be pursued as well as legal action.

3. College devices

Where possible, individuals should use College-owned computer equipment for work purposes so that minimum security requirements are met (e.g. encryption, automatic security updates and antivirus software).

Everyone must take the following steps:

- Only authorised staff should use College devices; protect login and password details even from family members;
- Do not make unauthorised changes to equipment (e.g. disabling antivirus or firewall software);
- Deploy software updates when requested by Technology;
- Return all equipment to Technology (e.g. laptops, tablets and USB storage) when leaving the College, including those purchased using research grants and log out of any personal services (e.g. Apple iCloud, Adobe Creative Cloud);
- Report lost or stolen devices to the Technology Service Desk immediately;
- Contact the Technology Service Desk when the device has problems or you notice the device not working as normal;

4. 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. Individuals must carry out appropriate due diligence to mitigate the increased risk of using their own devices, especially when working with confidential data. This means they:

- Enable disk encryption and protect with a strong password;
- Have a supported operating system with security updates regularly installed, including third-party applications (e.g. Adobe Acrobat);
- 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,
- Ensure devices do not contain software or services that could cause damage or harm to the College services, staff and student community;
- Follow the College's Acceptable Use Policy when using the device for work.;
- Not use personal email addresses to conduct college work.

Where a personal device is found to be non-compliant and a serious security risk, it may be blocked or restricted from accessing the RCA's computer systems and services.

5. Security best practice

- Enable auto-lock after a short period (e.g. 10 minutes).
- Avoid using public Wi-Fi to access College resources. Use the college Virtual

Private Network (VPN) or a secured wireless connection wherever possible.
- Avoid storing information on devices instead, use the shared drives provided. Where data must be stored on device, delete it when it is no longer required;
- Do not leave devices unattended in public spaces (e.g. coffee shops or trains).
- Be aware of your surroundings in public areas and consider buying a privacy screen if you regularly work with confidential information;
- Report any lost or stolen equipment as soon as is practicably possible to the Technology Service Desk;

6. Policy Review

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

7. 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)