Royal College of Art

Personal Device 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.

RCA has a responsibility to safeguard all information used and stored on behalf of the College. The College is committed to keep its data secure and to maintain compliance with the UK Data Protection Act 2018. This policy supports our commitment as part of the Data and Information Security policy suite.

RCA gives users of its services the choice to access its information using personal mobile phones. For the purpose of this document other personal devices such as laptops, home desktops, tablets, video and audio recording equipment are only allowed by exceptional circumstances.

However, the use of a personal devices poses information compliance and security risks such as:

- Loss or disclosure of confidential or sensitive information should the device be lost, stolen or has out of date security updates.
- Personal Devices storing RCA data making it difficult for the College and colleagues to find and retrieve necessary information
- Failure to comply with legal or contractual obligations such as providing access to information under DPA 2018.
- Compromising the security of Technology services.

2. Purpose & Scope

This policy sets out the College expectations regarding personal devices and the responsibilities for everyone who uses College resources, to ensure compliance with legislation and meet College security commitments. Its intent is to provide clear instructions on how personal devices can be used within the College.

This policy applies to all staff including third parties, contractors and consultants working on behalf of the college using a non-RCA managed device to process RCA data. All must adhere to these policies to keep the College and its people secure from Information security risks.

Whilst the Technology team will always endeavour to assist colleagues wherever possible, the team is not under any obligation to modify RCA systems or otherwise be responsible for issues arising with staff personal devices.

This document forms part of the College's data security toolkit and should be read in conjunction with other data and information security policies.

3. Policy Statements

The main requirement is that RCA's information and systems are protected from unauthorised access ensuring the confidentiality, integrity and availability of information.

Approved devices

- Each staff member with a contract greater than 0.3 FTE will be provided a college managed device for work purposes which will be maintained to meet the security standards required.
- Each staff member is limited to one device, if there is a need for a replacement then the older version device must be returned when receiving the newer device.
- Staff members shall ensure that the RCA managed device is returned at the end of their contract with RCA.
- Approved personal mobile devices accessing RCA data will be enrolled in RCA's mobile device management system to monitor (only) the security of the device operating system

Personal device security

- The responsibility lies with the individual to ensure that the appropriate controls are in place to mitigate the increased risk of using their own devices, especially when working with confidential and personal data.

- Laptop devices must be enabled with disk encryption and protected with a strong password.
- Devices must have a supported operating system with security updates regularly updated, including third-party applications. The device must not be used if the vendor no longer provides security updates.
- Devices must be enabled with auto-lock after a short period (e.g. 5-10 minutes).
- Devices must not be jailbroken (i.e. removal of software restrictions built into iPhones and other iOS devices).
- Devices must have anti-virus software installed which is updated regularly and a firewall running at all times.
- Devices must have a separate, secured account for work purposes, so others do not have access to confidential or sensitive information.
- Mobile devices must be implemented with a 6 digit pin code to unlock.
- Users shall not store RCA information on personal devices or personal cloud storage (e.g. Dropbox). Only RCA approved cloud storages should be used.
- Device security settings must be configured according to recommended security guidelines.
- Staff and students must have Multi-Factor Authentication enabled to access their RCA account.

Data governance

- Staff should be aware that RCA data held on personal devices might be subject to the Freedom of Information Act / Data Protection Legislation and must be processed in accordance with legislation including making RCA data accessible and retrievable to the College.
- Staff must avoid processing confidential, personal or sensitive personal data on personal devices, using College owned devices where possible.
- Staff must never store personal or sensitive personal data outside of their RCA account on their personal device. And it can be considered a criminal offence to take personal data that is not your own from an organisation (by emailing or downloading to a personal account).
- Staff must report any unauthorised access or loss of personal device used to access RCA data without delay and cooperate in any action to secure RCA information on the device.

- It is important for staff to report loss or unauthorised access as RCA is required to report data breaches to the information commissioner (ICO) within 72 hours of discovery.

4. Non-Compliance

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

5. Monitoring and Access

The College's Technology team will routinely monitor devices operating systems and antivirus software for non-compliance and if determined that a device is detrimental the security of the systems, Technology reserves the right to:

- Block a device from accessing RCA's network
- Block a device from accessing a particular system
- Take appropriate steps to retrieve or delete College information from the device

As a requirement of RCA's Cyber Essentials certification, personal mobile devices used to access RCA data will form part of the device checks verified by external assessors to ensure security updates are in place.

6. Key Related policies and processes

- Home and Remote Access to Services Policy.
- Information Security Policy.
- Account and Password Policy.
- Acceptable Use Policy.
- Data Protection Policy.
- Data security breach process (internal)