Royal College of Art

Information Security
Account and Password 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

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

This policy sets out the account and password requirements for anyone granted permission to use College Technology services (e.g. software, computers and network) and those responsible for managing them. The College operates on the principle of least privilege, and therefore only the appropriate level of access will be provided.

Non-compliance of policies puts people and the College at risk. A breach of information security may result in damage to you, our students, or your colleagues through the loss of control over personal data or confidential data, identity theft, fraud or financial loss. Breaches to this policy also put the College at risk of cyber-threats, legal action and regulatory penalties. Additionally, sometimes damages are irreparable and have serious reputational consequences.

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

3. Accounts and passwords

Passwords verify an individual's identity and allow access to a device, application or website and therefore maintains the confidentiality of systems and information. Consequently, they must remain secure and a secret (known only by the account owner).

Individuals given access to College Technology services will be issued a unique ID which may include an email address. It is their responsibility to take the following reasonable steps to protect them.

Accounts (e.g. name.surname@rca.ac.uk or name.surname.network@rca.ac.uk) must:

- be for the sole use of the individual issued to;
- not be shared with others;
- be activated with MFA;
- be logged out when finished;
- be deactivated at the end of the contract and removed after 6 months

In some circumstances, an individual delegates responsibility for managing another email account, but only with clear written permission from the owner. Delegation does not require sharing of account details, so please contact help@rca.ac.uk for assistance.

Passwords must:

- remain confidential, secure and unique. Never use the same password for both personal and College accounts.
- be changed if an account has been or is suspected of being compromised;
- be a minimum of 12 characters long and not contain easily identifiable names, pets, street addresses, birthdays, character strings such as ABC or simple keyboard patterns such as QWERTY
- not be easily guessed and should be passphrases made up of alphanumeric and special characters. Commonly used passwords such as Password123 are not acceptable.
- never be shared, not even with Technology.
- If individuals must write passwords down on paper, the note should be stored safely out of sight of others and kept secure at all times. However, writing passwords on paper is strongly discouraged and the use of password managers is encouraged.
- Use Multi-Factor Authentication (MFA) when accessing College systems and services, and not share the MFA applications or method (e.g. single-use password token generator etc.) with anyone.

Under no circumstances should an individual request someone’s password. If they do, signpost them to this policy and if they continue, report it to their line manager or Technology Service Desk. This includes being vigilant of requests for their account password through email and other means, and at no point should divulge their password when requested. Often external criminal elements use various means to trick individuals in order to gain access to their account.

4. High-risk accounts

System-level and privileged accounts such as those that allow users to carry out administrative tasks on an application pose a greater risk to College assets as they have extensive access to services and resources. Therefore additional steps are required:

Individuals must:

- Periodically at a minimum of every 3 months review privileged access and remove when no longer required;
- Temporary accounts must have an end date;
- Respect the rights of all users, the integrity of the systems and data;
- Use system or service accounts for scripts, services, password vaults or other automated processes;
- Use a separate standard account for daily use if responsible for a privileged account (e.g. local, domain administrator);
- Not use an administrator account to login, unless the purpose of the session is solely to make administrative changes;
- Not conduct any general web browsing or access email using a privileged account;
- Not use privileged access to make any changes that will compromise the security or integrity of a device, application or website;
- Where an account password (for services) is shared by a group of staff, use secure methods of storing passwords (e.g. password managers);
- Multi-Factor Authentication must be used to strengthen the login process.

5. Password and account security

- The setting of regular password expiration is not recommended by NCSC. Passwords should be changed if there is a possibility of compromise or it does not meet the password criteria;
- System accounts not used for a specific period (90 days) will be disabled;
- Account lockout policy will be implemented after 9th attempt of an unsuccessful login attempt;
- Privilege account passwords must be changed upon departure of the account owner;
- Default passwords for computer systems must be changed during installation;

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:

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