

Access Control Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	4
5. Formal Procedures for Allocating Access Privileges.....	4
6. Segregation of Duties.....	5
7. Use of Unique Accounts and Passwords.....	5
8. Use of Authentication Mechanisms other than Passwords	6
9. Allocation of Secret Authentication Information to Users	7
10. Password Management.....	7
11. Shared Accounts.....	8
12. Service Accounts.....	9
13. Generic Accounts.....	9
14. Privileged Access Accounts	9
15. Third-Party Support Accounts.....	10
16. Default Administrative Accounts	10
17. Temporary Accounts	11
18. Access Privileges for Databases Containing Sensitive Data.....	11
19. Remote Access	11
20. Non-Console Access.....	13
21. Console / Local Access	13
22. Access Logging and Monitoring.....	13
23. Review of Access Rights.....	13
24. Changes to Access Rights	13
25. Revocation of Access Rights.....	14
26. Cloud Services	14
27. Metrics and Reporting	15
28. Policy Review Date	15
29. Document Control	16
29.1 Document Revision History	16

1. Purpose

1.1. The purpose of this policy is to ensure that:

- All access to The Open College of the Arts (OCA)'s IT environment is controlled;
- All access is restricted to the least access privileges required to perform authorised job functions;
- Access privileges are reviewed at regular intervals;
- Access is removed as soon as there is no longer a requirement for such access;
- Authentication mechanisms, e.g. passwords, are securely controlled to prevent unauthorised access.

2. Scope

- 2.1. This policy applies to the OCA's IT networks and systems, regardless of where they are hosted and of whether they are provided and maintained internally or by third parties, including local and remote access requirements.

3. Policy Statement

- 3.1. The policy of the OCA in regard to access control is as follows:
- Access to all the OCA data and systems shall be controlled and monitored.
 - All access to systems and data shall be in accordance with the least privilege principle in that access is denied except where it is specifically required for functional purposes.
 - Access to data or systems that are not in the public domain shall be subject to a confidentiality agreement either in a contract or as a condition of engagement.
 - All system architecture, software and hardware shall be configured and controlled such that opportunities for unauthorised access or denial of service are minimised.
 - All access procedures shall be fully documented.
 - All users of information systems shall be authenticated and authorised. Authentication shall be, at a minimum, via the use of a password. Multi-Factor Authentication (MFA) shall be used for remote access (except under special circumstances) and access to cloud services.
 - All users shall be accountable for their actions on the OCA systems.

- Access control effectiveness shall be tested and measured through a formal program of penetration testing. This shall be controlled by the OCA and shall be conducted by a trusted third-party.

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- All the providers (internal or external) of IT systems and services to the OCA shall comply with this policy for the networks, systems, services and applications that they maintain.
- Business system owners shall comply with this policy for any information systems that they are responsible for managing. This shall include the management of access by staff and any relevant third parties.
- Business line management and information owners are responsible for approving, authorising and reviewing access to their respective resources, including related documentation of processes and procedures.
- Human Resources, all line managers and all staff shall facilitate implementation of this policy.
- Users are responsible for maintaining the security of their logon credentials and hardware keys.

5. Formal Procedures for Allocating Access Privileges

- Access management processes shall be documented and implemented, as applicable, by the IT Department, the providers of the systems/services and/or the business system owners.
- Access shall be granted to the OCA's IT networks and systems based on there being a business need for access. Users and IT administrators shall only be provided with access to network services that they have been specifically authorised to use.
- Role-based access control shall be implemented and centrally managed, through determining and documenting the access rights necessary for each role within the OCA to successfully carry out its assigned duties.
- All access privileges shall be assigned based on job classification, role and function. Access rights shall be restricted to the minimum necessary to perform a job role, based on a 'least privilege' principle.
- Access rights shall be controlled using pre-defined access profiles, based on job role and function.
- Access control mechanisms shall have a default 'deny-all' setting.
- All access requests, including new access requests and changes to access requests, shall only be granted where a formal request is raised and approved.

Each documented approval shall list the specific privileges that have been approved.

- Privileged access rights shall be:
 - Limited to the minimum number of roles required to have such access;
 - Granted for a time limited period and subject to review and reapproval to be renewed.
- Any privileged service account shall be local and shall not allow network login.

6. Segregation of Duties

- 6.1. Authorisation and approval procedures shall ensure there is appropriate segregation of duties in place to reduce the risk of accidental or deliberate misuse of the OCA's information and information processing facilities.
- 6.2. In line with these requirements, the following shall apply:
 - Access by business system managers and users shall be suitably restricted, e.g. with regards to financial applications.
 - Access by IT administrators shall be restricted as far as possible.
 - Access by software developers shall prevent them from accessing live systems without effective controls.

7. Use of Unique Accounts and Passwords

- Accounts shall not have designations that depict the purpose of the account login (e.g.: Backup, Admin).
- Accounts shall have application and technical owners who are responsible for the allocation and management of accounts and passwords.
- Access to information, systems and networks shall be controlled by the use of unique user accounts for both IT administrators and normal users. IT administrators shall use a unique IT administrator account for IT administration and a unique normal user account for all other work activities.
- Access shall only be allowed using a combination of a unique identifier and a unique password (or another unique authentication mechanism).
- Use of group, shared, or generic user accounts shall not be permitted for IT administrator and normal user activities. All default, generic accounts shall be disabled or removed when feasible; otherwise, the use of these accounts shall be blocked and prevented by strict access controls.
- Technical limitations may require the use of shared IT administrator accounts, e.g. root access for a UNIX system. In such cases, a unique IT administrator account

shall be used to instigate usage of the shared account¹ to ensure that access and usage of the shared account is traceable to an individual IT administrator.

- the OCA shall maintain inventories of all types of accounts and of authentication and authorisation systems in use.
- Where feasible, single sign-on (SSO) shall be implemented, together with MFA.

8. Use of Authentication Mechanisms other than Passwords

8.1. MFA² shall be enforced for:

- Remote access to the OCA's network and applications, unless an exception has been approved by the IT Manager for instances where this policy cannot be applied (e.g. for legacy systems);
- Access to cloud services.

8.2. MFA is not applicable to shared and/or service accounts (whether programmatic or individual person), but these accounts shall have additional compensating controls such as certificates and/or firewall policies to limit access.

8.3. MFA systems shall be phishing-resistant³ and configured to prevent misuse.

8.4. Where other authentication mechanisms are used, e.g. physical or logical security tokens, smart cards and certificates, use of these mechanisms shall be assigned as follows:

- Authentication mechanisms shall be assigned to an individual account and not shared among multiple accounts.
- Physical and / or logical controls shall be in place to ensure only the intended account and person(s) can use that mechanism to gain access.
- Where service or other shared accounts are used and/or approved the above additional authentication mechanisms shall be enforced.

8.5. Where feasible, equipment identification shall be used as a method for connection authentication.

¹ E.g. via the 'sudo' command, or an IT administrator could login via an intermediate bastion host or jump box with associated logging and monitoring.

² Note that using one factor twice, e.g. using two separate passwords, is not considered MFA.

³ Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure.

9. Allocation of Secret Authentication Information to Users

- 9.1. The allocation of secret authentication information, e.g. passwords, shall be controlled through a formal management process. The IT Department and business system owners shall ensure that the correct user is provided with the secret authentication information and that there is no risk of an unauthorised person obtaining the secret authentication information.

10. Password Management

- 10.1. All users, IT administrators and business system owners shall comply with the following password management requirements⁴. These settings shall, where feasible, be enforced by system and application controls.
- All accounts shall use passwords that are at least 14 characters in length.
 - Passwords shall be difficult to guess. The following two approaches are valid for this:
 - One possible approach is to adopt user-generated passwords that follow the 'three random words' rule, where the password is composed of the concatenation of three random words, chosen to make the password easy to memorise for the user but difficult to guess by an attacker. This approach shall be used for the main account of the user.
 - An alternative approach is to use machine-generated passwords, generated by an approved password manager, with built-in complexity rules. This shall be reserved for the case when users need to have separate accounts (without SSO) for some systems, and the password manager should be used systematically by the user to copy-paste the securely stored passwords directly into the relevant login pages, without having to memorise (or even know) those passwords.
 - Passwords shall not be set to expire after any defined period.
 - Whenever a password is known or suspected to have been compromised, this shall be immediately communicated to the IT Department and the password shall be immediately changed.
 - When a password needs to be changed, the last 12 passwords shall not be re-used.

⁴ These requirements are aligned to the National Cyber Security Centre (NCSC) best practice guide to password management. This guidance replaces the deprecated approach of using complexity and expiry rules.

- A normal user account shall be locked out after 6 failed logon attempts. The lockout duration shall be at least 30 minutes or until an authorised IT administrator unlocks the account.
- An IT administrator account shall be locked out after 2 failed logon attempts until an authorised IT administrator unlocks the account.
- Passwords shall be stored securely.
- Stored passwords shall be hashed using strong cryptography in line with current security industry best practice.
- Transmitted logon credentials shall be encrypted using strong cryptography in line with current security industry best practice.
- Logon procedures shall not display a password or password characters when it is being entered.
- If first time passwords are configured by IT administrators for users, then these passwords shall be unique per user, and they shall need to be changed upon first logon. The same also applies for any password resets.
- Unsuccessful logons shall result in disconnection with no assistance. There shall not be any indication of which part of the logon data is in error, i.e. the user ID or password.
- A user's identity shall be verified before password resets are performed. Secure methods shall be implemented to ensure that remote users' identities are adequately verified.
- Where feasible, technical controls shall be used to manage the quality of passwords.
- Inactive sessions shall be terminated after a defined period of inactivity of no more than 15 minutes.

11. Shared Accounts

- 11.1. In certain circumstances it may be necessary and unavoidable due to business need or technical constraints for an account privilege to be shared amongst multiple users.
- 11.2. The following shall apply to shared accounts:
 - The business owner of the solution or service shall be the owner of any shared accounts.
 - Any shared accounts shall be created with a recorded exception.
 - Shared accounts shall be subject to periodic review.

- Any available audit data shall be retained for shared account login.
- Shared accounts with privileged access shall be subject to the same controls and audit as any other privileged account.

12. Service Accounts

- 12.1. Service accounts may be required where a technology mandates a specific capability, access or naming for an application or service and shall only be used for approved and specific business technical needs.
- 12.2. The following shall apply to service accounts:
 - The technical owner of the solution or service shall be the owner of any service accounts.
 - They shall be uniquely named to the host where the service resides.
 - They shall have local system login only and not be accessible from the network.
 - They shall be approved by the technical owner.
 - Service accounts with privileged access shall be subject to the same controls and audit as any other privileged account.
 - They shall not be mandated to have MFA, but it is strongly recommended that additional controls are applied.

13. Generic Accounts

- 13.1. Generic accounts may be required where a technology mandates a specific capability or naming for users or roles and shall only be used for specific business application needs.
- 13.2. The following shall apply to generic accounts:
 - There shall be a documented business owner of the solution or service for any generic accounts.
 - They shall be uniquely named to the host where the service resides.
 - They shall be approved by the application owner.
 - They shall have additional controls and audit where MFA is not technically feasible.
 - Generic accounts with privileged access shall be subject to the same controls and audit as any other privileged account.

14. Privileged Access Accounts

- 14.1. Privileged access accounts are those accounts such as administrator, maintenance and support accounts which have a higher level of privilege than the standard user account for a system or service.
- 14.2. The following shall apply to privileged access accounts:

- They shall be restricted to the minimum number of users required to have such access, in line with the least privilege principle.
- They shall be granted for a time limited period and subject to review and reapproval to be renewed.
- There shall be a business and technical owner of the solution or service for any privileged accounts.
- Their username and/or password shall be changed from the operating system (OS) or application default (e.g. admin/administrator).
- They shall be accessed through Privileged Access Management (PAM) capability.
- They shall be auditable and recorded.
- They shall require an approved non-privileged account to increase privilege from.
- The association with the named user account to the privileged account shall be recorded.
- They shall use MFA for privileged access or prior to privilege escalation; this should be undertaken through a PAM tool.

15. Third-Party Support Accounts

- 15.1. Third-party support accounts are those accounts for partners and suppliers to access specific the OCA systems or services;
- 15.2. Where technically feasible the following shall apply to third-party support accounts:
 - They shall be disabled when not in use.
 - They shall have MFA applied.
 - There shall be a business owner of the solution or service for any third-party support accounts.
 - Third party accounts with privileged access shall be subject to the same controls and audit as any other privileged account.

16. Default Administrative Accounts

- 16.1. Default administrative accounts are those accounts who have known/recognised default account details, e.g. Admin/Administrator, root/password where the username and/or password cannot be changed.
- 16.2. Where technically feasible the following shall apply to default administrative accounts:
 - They shall have additional controls and audit where MFA is not technically feasible.

- Default administrative accounts with privileged access shall be subject to the same controls and audit as any other privileged account.
- Where the default administrative account details cannot be changed, compensating controls shall be applied to protect access to the known account.

17. Temporary Accounts

- 17.1. Temporary accounts are those accounts that are created for a specific short-term purpose.
- 17.2. The following shall apply to temporary accounts:

- They shall be approved by the technical and business owner.
- They shall be time bound with an approved period before being disabled.
- They shall be disabled after 7 days if no validity period is set on creation.
- Enabling and disabling of account shall be recorded and auditable.
- Temporary accounts with privileged access shall be subject to the same controls and audit as any other privileged account.

18. Access Privileges for Databases Containing Sensitive Data

- 18.1. All access (including access by applications, administrators and all other users) to any database containing sensitive data, e.g. personal data, cardholder data or commercial data, shall be restricted as follows:
- All user access to, user queries of, and user actions on databases shall be through programmatic methods.
 - Only database administrators shall have the ability to directly access or query databases.
 - Application IDs for database applications shall only be used by the applications (and not by individual users or other non-application processes).

19. Remote Access

- The standard method of remote access from an external source to the OCA data and systems is via the Internet using cryptographic and authentication methods appropriate to the degree of access required and the classification of the information to be accessed. (See the [Information Classification and Handling Policy](#) for details.)
- Only the OCA approved and/or provided remote access methods shall be used. Remote access from outside of the OCA's corporate network shall incorporate the use

of MFA, e.g. a password and a software token plus Virtual Private Network (VPN) access.

- For remote access to applications:
 - MFA shall be used for any publicly facing gateway in addition to any OS and application login requirements, where applicable.
 - All non-local administrative accounts shall have MFA enabled.
 - The initial connection shall be made by establishing a connection over the Internet using the latest version of a VPN or equivalent secure communications channel to an OCA server in a Demilitarised Zone (DMZ). Once authenticated, the encrypted session shall continue until the user disconnects or times out due to inactivity.
 - The functionality within the environment shall be controlled by the application based on the least privilege principle.
 - Any banner information presented upon connection to the Internet shall be removed and replaced with an unobtrusive login prompt which includes a warning relating to unauthorised access. The warning shall also clearly communicate to the user that their activities on the network will be monitored and that by logging on the user grants permission for such monitoring.
 - The banner shall not disclose company name, or any context of the connected gateway.
- For direct remote access to the network:
 - Connectivity shall be via a secure approved client VPN installed on the user device (which shall be the OCA domain connected or a device which has been given prior written approval).
 - Initial connection to the the OCA firewall is by a connection to the Internet and then establishing a VPN session.
 - MFA shall be used at the publicly-facing gateway in addition to any OS and application login requirements, where applicable.
 - The VPN shall be configured such that the session terminates automatically after a set period of inactivity.
- All remote access sessions shall be automatically disconnected after a specified period of inactivity.
- All third-party access shall only be granted when required and shall be monitored.
- All third-party identities managed by the OCA shall be clearly distinguishable from any the OCA internal employee or contractor, and not be assigned an OCA primary domain or identity.

- All remote access architecture shall be configured such that access and user identity management activity is monitored and logged via an OCA approved capability or third-party so that unusual activity such as failed login attempts and abnormal, unusual usage patterns can be identified.

20. Non-Console Access

20.1. Non-console access by IT administrators shall:

- Incorporate use of MFA;
- Be encrypted using strong cryptography, in line with the [Cryptographic Controls Policy](#).

21. Console / Local Access

- 21.1. All consoles when not in use shall be logged out and require administrative privilege account to login.
- 21.2. All consoles shall avoid identifying data on screen when signed out. No indication of ownership or purpose shall be included on the physical devices or local login console.

22. Access Logging and Monitoring

- 22.1. All access events relating to any the OCA networks, systems and applications shall be logged and regularly monitored. See the [Logging and Monitoring Policy](#) for further details.

23. Review of Access Rights

- 23.1. All access privileges shall be subject to regular review on a quarterly basis, including access to networks, operating systems, applications, services and software. The IT Department shall review access in line with this requirement, whilst business system owners shall specifically review access to the systems that they are responsible for.
- 23.2. Whenever temporary access is granted, the access shall be revoked within a formally defined time period.

24. Changes to Access Rights

- 24.1. All changes to access rights shall only be granted where a formal request is raised and approved. Each documented approval shall list the specific privileges that have been approved, and / or those that have been revoked.

- 24.2. Line managers shall ensure that the IT Department and all relevant business system owners are notified of any required changes in access rights.

25. Revocation of Access Rights

- The IT Department and business system owners shall ensure that user accounts are deactivated after 45 days of inactivity.
- Line managers, with the assistance of Human Resources, shall ensure that the IT Department and all relevant business system owners are notified of any requirements for revoking access rights, e.g. when an employee moves within or leaves the OCA. See the Joiners, Movers and Leavers Procedure for details.
- Revocation of access rights shall only be managed via a formal request. Each processed request shall list the specific privileges that have been revoked and the user accounts that have been disabled or removed.
- When an employee leaves the OCA, the line manager shall be responsible for ensuring that all the OCA assets, such as PCs, laptops, mobile phones and physical security access devices / badges are returned to the OCA.
- When an employee takes an extended leave of absence from the OCA, the line manager shall be responsible for ensuring that all assets are recorded. Dependant on circumstance:
 - Each asset shall be returned until such time as the employee returns to the business or leaves;
 - Security access devices / badges shall be returned until such time as the employee returns to the OCA;
 - Access to the OCA internal networks and services shall be suspended;
 - Access to the employee the OCA data shall be made available to their line manager.

26. Cloud Services

- 26.1. Where the OCA uses cloud services, the responsibilities for access control can be shared between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC), in line with the Shared Security Responsibility Model⁵.
- 26.2. In all cases, the split of responsibilities shall be clearly documented in contractual terms.

27. Metrics and Reporting

- 27.1. Relevant metrics for access control shall be defined, and regularly obtained and reported to the Finance, Employment, Audit and Risk (FEAR) Committee.

⁵ See [Cloud Security Policy](#).



The Open College of the Arts



The Open
University

- 27.2. Analysis of metrics shall be used to assess the efficiency of the access control processes and continuously improve them.

28. Policy Review Date

- 28.1. This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.

29. Document Control

Document Control

Title:	Access Control Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

29.1 Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	05/11/2025	Dean Humphreys	Final revisions approved and version updated to 1.0 for release