

Asset Management Policy

Table of Contents

1. Purpose	3
2. Scope.....	3
3. Policy Statement.....	3
4. Roles and Responsibilities	4
5. Asset Ownership	4
6. Asset Register.....	5
6.1 Generalities	5
6.2 Logical Assets	6
6.3 Physical Assets	6
7. Use of Assets.....	7
8. Asset Disposal	8
9. Metrics and Reporting	8
10. Policy Review Date	8
11. Document Control	9
11.1 Document Revision History	9

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate the requirements for the management of all the Open College of the Arts (OCA)'s information and IT assets (logical or physical).
- 1.2. This policy is independent of any hardware and software environment and shall be used as a generic baseline for the management of any kind of assets.

2. Scope

- 2.1. This policy applies to the OCA's information and IT assets, whether logical or physical.
 - Logical assets include:
 - Software assets;
 - Information assets in any format, including but not limited to databases, files and documents.
 - Physical assets include all IT hardware, including but not limited to:
 - Servers, PCs, network devices and mobile devices;
 - Communication equipment;
 - All media storage devices including portable devices;
 - Physical access control and authentication devices including tokens;
 - Non-computing / Internet of Things (IoT) devices;
 - Operational Technology (OT) devices;
 - Devices that are regularly connected to the OCA's network infrastructure, even if they are not under control of the OCA.
 - This policy applies to assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments.
- 2.2. This policy applies to all the OCA staff (including employees, temporary staff, contractors, consultants and partners), and any third parties who help the OCA provide its services.

3. Policy Statement

- 3.1. The policy of the OCA in regard to asset management is as follows:
 - All assets shall be classified according to the [Information Classification and Handling Policy](#).
 - All assets shall be subject to a risk assessment on acquisition and as part of the ongoing management of the asset.
 - All assets shall have a designated owner.
 - All assets shall be accounted for and recorded in an asset register.

- The asset register shall be regularly audited and validated.
- Processes shall be defined and documented for the acquisition, management, ownership and disposal of assets.
- All assets shall be subject to appropriate security controls throughout their lifetime.
- Security requirements for the management of each asset shall be specified in policies and/or standards for the corresponding subject area, as applicable.
- All losses, thefts or compromise of assets shall be investigated and resolved in line with the [Information Security Incident Response Policy](#).

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- The IT Department is responsible for maintaining an up-to-date asset register of all information and IT assets that belong to the OCA.
- Asset owners are responsible for the implementation and maintenance of appropriate controls throughout the lifetime of the asset. This includes:
 - Classification of the asset in accordance with the [Information Classification and Handling Policy](#);
 - Control of access to the asset in accordance with the [Access Control Policy](#);
 - Disposal of the asset in accordance with the [Information Classification and Handling Policy](#);
 - Communication to the IT Department of any changes to the asset that might need to be updated in the asset register.
- The IT Manager and line managers are responsible for:
 - Implementing a process of maintaining asset ownership and ensuring that ownership responsibilities are assigned;
 - Conducting audits that validate the asset register.
- All the OCA staff shall comply with this policy and facilitate its implementation.

5. Asset Ownership

- 5.1. Ownership shall be assigned when assets are created in or acquired by the OCA. The identified asset owner shall be either an individual or team that has the responsibility, approved by management, for controlling the whole lifecycle of the asset.
- 5.2. The owner of an asset shall:

- In the case of an information asset, assign a classification to the asset, in line with the [Information Classification and Handling Policy](#);
 - Ensure that the asset is inventoried in the asset register, by providing the necessary information to the IT Department (see section 6 below);
 - Ensure that access to the asset is controlled, and provided strictly on a need-to-know basis, in line with the [Access Control Policy](#);
 - Ensure that, when an information asset needs to be disposed of, this is done in line with the [Information Classification and Handling Policy](#);
 - Ensure that, when they cease to have the responsibility for an asset, ownership is properly passed to the new designated owner.
- 5.3. Asset owners shall not have any property rights to the assets, as these belong to the OCA.
- 5.4. Assets may be allocated to custodians for use. In such cases, the asset owners shall remind the appointed custodians of their responsibility to comply with the relevant OCA policies.

6. Asset Register

6.1. Generalities

- 6.1.1. The IT Department shall maintain an up-to-date asset register of all information and IT assets that belong to the OCA.
- 6.1.2. The asset register can consist of one or more inventories: it is acceptable to maintain separate inventories for different types and categories of assets (logical and physical).
- 6.1.3. Asset owners shall communicate to the IT Department any relevant information for the creation or update of the corresponding records in the asset register.
- 6.1.4. Access to the asset register shall be restricted on a need-to-know basis.
- 6.1.5. Appropriate tools shall be in place to automate, as much as possible, the discovery of assets and the update of the asset register, e.g.:
- Active/passive asset discovery tools;
 - Dynamic Host Configuration Protocol (DHCP) logging;
 - Automated software inventory tools.
- 6.2. The asset register shall be subject to regular audits, under the responsibility of the IT Manager and/or relevant line managers, to validate that it is fit for purpose and up to date. Any assets found to be out of support shall be reported and addressed.
- 6.3. The following details shall be recorded for all assets:
- Type;
 - Name;
 - Purpose;
 - Owner;

- Unique ID reference;
- Date of acquisition/implementation (as applicable);
- Criticality for the business;
- Status;
- Custodian(s) (if applicable);
- Date of decommissioning / disposal (if applicable);
- Secure configuration information (if applicable).

6.4. Other details applicable to the different categories of assets are listed in the subsections that follow.

6.5. Logical Assets

6.5.1. The following details shall be recorded for software assets:

- Supplier;
- Version;
- Date of acquisition (or implementation, if internally developed);
- Uniform Resource Locator (URL) (if applicable);
- App store (if applicable);
- Deployment mechanism;
- License details (if applicable);
- Expiry / renewal date (if applicable);
- End-of-life support date (if applicable).

6.5.2. The following details shall be recorded for information assets:

- Classification;
- Version;
- Author;
- Format;
- Location of master copy.

6.6. Physical Assets

6.6.1. The following details shall be recorded for physical assets:

- Supplier;
- Make;
- Model type;
- Model number;
- Serial number;
- Date of acquisition;
- Location of usage;
- End-of-life support date;

- Network address (if static);
- Machine address;
- Whether the asset has been approved to connect to the network;
- Instruction manual;
- Maintenance interval;
- Maintenance budget code;
- Maintenance plan location.

7. Use of Assets

- 7.1. Assets shall only be used for the business purpose for which they are intended, under the appropriate approval and authority, and in compliance with the relevant the OCA policies. Detailed requirements for the acceptable use of information, assets associated with information and information processing facilities are contained in the [Acceptable Use Policy](#).
- 7.2. Only currently supported assets shall be considered as authorised. If software is unsupported, yet necessary to fulfil the OCA's objectives, an exception detailing mitigating controls and residual risk acceptance shall be documented. Any unsupported software without an exception documentation shall be designated as unauthorised. There shall be a review of the software list to verify software support at least monthly, or more frequently.
- 7.3. Unauthorised assets shall be reviewed and addressed on a weekly basis. the OCA may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.
- 7.4. Technical controls shall be in place to ensure that only authorised software / libraries / scripts are allowed to be executed / used in business processes.
- 7.5. Where applicable, requirements for the use of specific types of assets may be covered in other the OCA policies and/or standards.
- 7.6. Information assets shall be handled according to their classification, in line with the [Information Classification and Handling Policy](#).
- 7.7. All losses, thefts or compromise of assets shall be investigated and resolved in line with the [Information Security Incident Response Policy](#).

8. Asset Disposal

- 8.1. Assets shall be disposed of securely, in compliance with the relevant OCA policies.
- 8.2. The disposal of information assets shall be done in compliance with:
 - The [Information Classification and Handling Policy](#), according to their classification;
 - The [Data Retention and Disposal Policy](#).

- 8.3. The secure disposal of physical assets (including equipment and storage media) shall ensure:
- Equipment is verified to confirm that any Non-Public information and licensed software has been securely removed, as relevant, prior to disposal or re-use.
 - Storage media containing Non-Public information shall be physically destroyed or the information shall be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using a standard delete or format function.
- 8.4. Related policy requirements are documented in the [Information Classification and Handling Policy](#).
- 8.5. When assets are disposed of, their status shall be appropriately updated in the asset register to reflect this.

9. Metrics and Reporting

- 9.1. Relevant metrics for asset management shall be defined, and regularly obtained and reported by the IT Manager to the Finance, Employment, Audit and Risk (FEAR) Committee and OCA Board as appropriate.
- 9.2. Analysis of metrics shall be used to assess the efficiency of the asset management process and to drive its continuous improvement.

10. Policy Review Date

- 10.1. 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.

11. Document Control

Document Control	
Title:	Asset Management Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

11.1 Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	06/11/2025	Dean Humphreys	Final revisions approved and version updated to 1.0 for release