

Backup and Recovery Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	3
5. Backup and Recovery Requirements	3
6. Cloud Services	5
7. Metrics and Reporting	5
8. Policy Review Date	5
9. Document Control	6
9.1 Document Revision History	6

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate the requirements for backup and recovery of The Open College of the Arts (OCA)'s IT systems, and to ensure that backup and recovery procedures and technology are in place to protect the OCA from losses or corruption of information, software or systems, e.g. due to unauthorised changes to information and software, technical failures, viruses and fire.

2. Scope

- 2.1. This policy applies to all the OCA electronic information, software and systems which require backup and recovery facilities.
- 2.2. The OCA's organisation-wide business continuity requirements, plans, procedures and solutions are addressed in the Business Continuity Policy.

3. Policy Statement

- 3.1. The OCA's policy in regard to backup and recovery is that appropriate procedures and technology shall be in place to enable the OCA to fully recover from losses or corruption of information, software or systems.

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- Business system owners are responsible for defining backup and recovery requirements, based on legal, statutory, regulatory, contractual and business requirements for information retention.
- The IT Department is responsible for defining backup and recovery procedures, and identifying, implementing and maintaining solutions that support the OCA's backup and recovery requirements.
- Software developers are responsible for ensuring that any source code that is owned by the OCA is backed up on a regular basis.
- All staff are responsible for ensuring that any information that they create, or change is backed up on a regular basis. This shall be achieved by ensuring that information is stored on the OCA's approved locations.

5. Backup and Recovery Requirements

- Business system owners shall define requirements for information backups, on a per information system basis, via formal business impact assessments. In this way, the criticality of the information shall be determined, which in turn shall dictate the requirements for backup, retention and recovery in terms of:

- What needs to be backed up;
 - The frequency of backup, e.g. daily or weekly;
 - Whether full or partial backups, or snapshots, are needed;
 - Whether encryption of backups is required, i.e. for the secure storage of sensitive information such as personal or commercial information;
 - Secure storage and availability to authorised individuals of encryption passphrases or certificates/key data for recovery from backup onto newly installed resources if required;
 - The period of time the information needs to be retained – this shall be aligned to the Data Retention and Disposal Policy;
 - The Recovery Time Objective (RTO);
 - The Recovery Point Objective (RPO);
 - Whether offline backup capabilities need to be considered to protect against ransomware or similar attacks.
- Software developers shall engage with the IT Department to ensure that all changes to source code and managed secrets / vaults are backed up on the day of the changes.
 - The IT Department shall identify, implement and maintain suitable backup and recovery solutions for the OCA's electronic information, software and systems. By default, all backups shall be made to a storage repository with robust security controls, which protect the backup copies. The adequacy of the backup and recovery solutions shall be reviewed on at least an annual basis.
 - All critical systems shall be backed up on at least a daily basis. Backups for critical systems shall be formally scheduled to run at the most appropriate time, i.e. a quiet processing time outside of normal operating hours.
 - All critical cloud-based services for which the OCA is responsible for backup and recovery shall be backed up / have recoverable image snapshots taken on at least a daily basis. These backups shall be formally scheduled to run at the most appropriate time, i.e. a quiet processing time outside of normal operating hours.
 - All critical systems / services shall be backed up / have a snapshot taken at an appropriate point before any significant / major new deployment, to support rollback in the event of issues with deployment or operation of new versions of system or service.
 - All infrastructure configuration if not backed up as part of the requirements above shall be securely backed up and stored.
 - Accurate and complete records of the backup copies shall be maintained, and inventory records shall be reviewed at least annually.
 - Operational processes shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups. The IT Department shall ensure that suitable alerting and response facilities are in place.
 - The backups shall be stored in remote locations, at a sufficient distance to escape any damage from a disaster at the site which hosts the systems that are backed up.

- The security of off-site storage locations shall be reviewed at least annually. Backups shall be given an appropriate level of physical and environmental protection consistent with the standards applied to the source information.
- The transportation of backups and where backups are located shall be logged within backup media inventories. The transport of all backup media shall be authorised by management and sent via secure courier services or other delivery method that can be tracked.
- Documented recovery procedures and recovery testing schedules shall be maintained and exercised by the IT Department and relevant business system owners.
- Where used, backup media shall be regularly tested to ensure that it can be relied upon for emergency use when necessary. Testing the ability to restore backups shall be performed onto dedicated test media, and not by overwriting the original media in case the backup or restoration process fails and causes irreparable damage or loss.
- Where specific hardware is required to recover backups, availability and compatibility of said equipment shall be validated on an annual basis.
- Methods required for the destruction of backup media when it is no longer required, or becomes unusable.
- Where systems or services involving the OCA information are delivered by cloud providers, they shall include backup and recovery capabilities in line with the requirements above.

6. Cloud Services

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

7. Metrics and Reporting

- 7.1. Relevant metrics for backup and recovery shall be defined, and regularly obtained and reported to the Finance, Employment, Audit and Risk (FEAR) Committee and OCA Board as appropriate.
- 7.2. Analysis of metrics shall be used to assess the efficiency of the backup and recovery processes and continuously improve them.

8. Policy Review Date

- 8.1. 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.

9. Document Control

Document Control	
Title:	Backup and Recovery Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

9.1 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