

Information Security Management System (ISMS) Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Context of the Organisation	3
4. Information Security Risk Management	4
5. Performance Evaluation	4
6. Improvement	5
7. Roles and Responsibilities	5
7.1. RACI Matrix.....	6
7.2. Interested Parties	6
7.3. Internal Parties	6
7.4. External Parties	7
8. Policy Review Date	7
9. Compliance and Exceptions	8
10. Document Control	8
10.1 Document Revision History	8

1. Purpose

The purpose of this Information Security Management System (ISMS) policy is to define a systematic approach for establishing and maintaining an ISMS, protecting the confidentiality, integrity, and availability of information assets within the Open College of the Arts (OCA). This policy ensures compliance with applicable regulations, enhances risk management and safeguards data from security threats.

Our ISMS provides a structured framework for identifying, assessing, and mitigating security risks while fostering a culture of continuous improvement and security awareness. Through effective governance, policies and controls, we ensure that information security remains a fundamental priority in achieving our strategic objectives.

2. Scope

This policy applies to all OCA employees, contractors, consultants, suppliers and other interested third parties that have access to OCA's information. It covers all digital and physical information assets owned, managed or processes by the college, including records, data and IT infrastructure.

3. Context of the Organisation

- The OCA is an independent organisation endorsed and supported by the Open University. The college's head office in Barnsley provides a managed private network for employees' use, which is managed and maintained by Barnsley Metropolitan Borough Council (BMBC). Internal IT services including desktop services, support, information security and vendor management are the responsibility of the IT Team, which sits within the Technology and Innovation department.
- OCA has assessed the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of its ISMS. More details can be found in the roles and responsibilities section of this document.
- The following business functions within OCA are in scope for the ISMS:
 - HR
 - Finance
 - Student Services
 - Learner Support
 - Technology Enhanced Learning
 - IT Services
 - Marketing
- The following locations are in scope for the ISMS:
 - The Michael Young Arts Centre, Room 301, DMC 02, County Way, Barnsley, S70 2AG

- The OCA shall implement, maintain and continuously improve, an ISMS following the Plan-Do-Check-Act (PDCA) cycle to enhance information security, risk management and continuous improvement. The OCA shall plan by identifying opportunities, do by implementing changes, check by evaluating results against expectations, and act by adjusting and standardising successful practices, ensuring that the ISMS is aligned to business needs, security objectives and resilience goals.

4. Information Security Risk Management

- The OCA's top management shall establish and implement an [Information Security Policy](#) aligned with strategic objectives, supported by related policies, standards, and procedures. With a commitment to integrating ISMS into business processes, guiding staff, and promoting continuous improvement. The Information Security Committee shall oversee the ISMS implementation, ensuring adequate resources for the ISMS, including staff competence and training, policy awareness, relevant communication, and comprehensive documentation.
- Risks and opportunities shall be identified and managed through a risk management framework, with controls selected per ISO 27001:2022 as well as bespoke controls, where relevant. Objectives shall focus on confidentiality, integrity, and availability of information, with actions, resources, responsibilities, and evaluation mechanisms in place.
- The OCA shall plan, implement, and control both internal and outsourced processes to meet ISMS requirements and achieve information security objectives. This includes maintaining documented information to ensure processes are carried out as planned, managing planned changes and reviewing unintended changes to mitigate adverse effects in line with the [Change Management Policy](#). Additionally, the OCA will perform and document information security risk assessments at planned intervals or when significant changes occur and implement and document the risk treatment plan in accordance with the [Information Security Risk Management Policy](#).

5. Performance Evaluation

- The OCA shall monitor, measure, analyse, and evaluate the ISMS's performance and effectiveness by identifying what needs to be monitored, selecting appropriate methods to ensure consistent results, determining the frequency and responsibilities for these activities, and maintaining documented evidence of the results.
- The OCA shall conduct internal audits of the ISMS at planned intervals to ensure compliance with the OCA requirements, and to verify effective implementation and maintenance. This involves planning, implementing and maintaining an audit program that considers process importance and past audit results, defining audit criteria and

scope, selecting impartial auditors, reporting audit results to the Information Security Group (ISG), and retaining documented evidence of the audit program and results.

- The ISG shall conduct management reviews of the ISMS at planned intervals to ensure its suitability, adequacy, and effectiveness. These reviews shall consider the status of previous actions, changes in relevant issues, performance feedback (including control deviations, monitoring results, audit results, and security objectives), feedback from interested parties, risk assessment results, and improvement opportunities. The outcomes, including decisions on continual improvement and necessary changes to the ISMS, shall be documented.

6. Improvement

- The OCA shall continually improve the suitability, adequacy and effectiveness of the ISMS, incorporating the outcomes of the evaluation of its performance.
- OCA shall evaluate and take appropriate action to correct for any control deviation that is identified in the ISMS. Control deviations are typically identified as part of the monitoring and evaluation of the performance of the ISMS but can also be identified through other means on the day-to-day operation of the ISMS.
- Actions taken shall be appropriate to the effects of the control deviations encountered and appropriately documented.

7. Roles and Responsibilities

- The Finance Employment, Audit and Risk Committee (FEAR) is responsible for:
 - Approving this policy and shall ensure that this policy is up-to-date and relevant.
 - The implementation and management of the ISMS and for ensuring that it achieves OCA's information security objectives and operates effectively, reporting to the OCA Board
- The IT Manager:
 - Maintains ownership of this policy, has responsibility for the day-to-day operation of the ISMS, for monitoring its performance, reviewing and reporting policy changes to the FEAR Committee for their approval.
- Line managers are responsible for:
 - Ensuring that the areas under their responsibility comply with the requirements of the ISMS and contribute to its performance.
 - Ensuring that their staff comply with this policy.
- All OCA employees, contractors, consultants, suppliers and other interested third parties that have access to OCA's information have the responsibility to comply with the requirements of the ISMS within this policy.

7.1. RACI Matrix

Activity / Responsibility	Information Security Group (ISG)	FEAR Committee	IT Manager	Line Managers	Employees, Contractors & Third Parties
Approve and update the policy	A	R	A	C	I
Implement and manage the ISMS	R	I	A	C	I
Ensure the ISMS meets security objectives	A	I	R	C	I
Own and maintain the policy	C	I	R	I	I
Monitor ISMS performance	C	I	R	I	I
Review and report policy changes	C	I	R	I	I
Ensure compliance with responsible areas	I	I	C	R	I
Ensure staff comply with policy	I	I	C	R	I
Comply with ISMS requirements	I	I	I	I	R

Key: R = responsible, A = accountable, C = consulted, I = informed.

7.2. Interested Parties

The OCA has identified the interested parties that are relevant to the information security management and the needs and expectations of those interested parties, listed below. They shall be regularly reviewed and reassessed when changes occur, to ensure that they are understood and appropriately addressed in the operation of the ISMS, and that all associated risks, opportunities and issues which may affect the effectiveness of the ISMS are identified.

7.3. Internal Parties

Description	Needs / Expectations
The OCA Board	Implementation of an ISMS supports the OCA Board's vision of successfully delivering and expanding services.
FEAR Committee	- Delivery of the ISMS is seen as an enabler to help meet the expectation of existing and potentially new students. - Addressing operating environment requirements from regulators. - Expects a return in the investment of security related resources – staff, processes and technology.

Description	Needs / Expectations
Information Security Group (ISG)	Implements the ISMS and associated policies, standards and procedures in support of meeting the ISMS security objectives. Supports the review and maintenance of the ISMS and associated policies, standards and procedures. Monitors and reviews OCA compliance with the ISMS security objectives.
IT Manager	• Performance and day-to-day operation of the ISMS. • Identification of enterprise-wide IT infrastructure and security requirements to be included in the ISMS scope. • Identification and deployment of technology to support operations.
Line Managers	• Deployment of the ISMS in a timescale that supports business objectives. • Security framework activities delivering assurance expected by students and staff • Providing sufficient resources to help maintain the expansion of ISO 27001:2022 control objectives to meet new business services where necessary. • Recruiting staff with the necessary level of skills to deliver and support the ISMS. • Deployment of shared technology, with embedded security, to facilitate business opportunities.
IT Team	• Supporting OCA's business requirements with regards to IT needs, e.g. networking and computing devices.
Staff	• Expectation that the ISMS shall support business requirements across all locations.

7.4. External Parties

Description	Needs / Expectations
Regulatory Bodies	• Compliance with applicable legislation and regulations.
Suppliers ¹	• Continued business relationship. • Compliance with information security requirements.
Students and Customers	• Availability of services. • Confidentiality and robust access controls.

¹ Including Cloud Service Providers (CSPs).

Description	Needs / Expectations
	Maintenance of required certifications.

8. Policy Review Date

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, or any other significant changes in the organisation or its context that may dictate the need for an update.

9. Compliance and Exceptions

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

Exceptions to this policy must be submitted in writing and approved by the policy owner. Exceptions shall be risk assessed on a case-by-case basis, include a valid justification and recorded in the risk register.

10. Document Control

Document Control	
Title:	Information Security Management System (ISMS) Policy
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager, Dean Humphreys
Approver:	FEAR Committee
Classification:	Internal
Next Review Date:	October 2026

10.1 Document Revision History

Version	Date	Author	Summary of changes	Approver
0.1	04/10/2024	D. Horrocks	Initial draft	
0.2	28/01/2025	B. Bayliff	Addressed comments from first review (received 27/01/2025)	
0.3	06/02/2025	B. Bayliff	Addressed comments from second review and meeting	



The Open College of the Arts



The Open
University

			with Dean on 05/02/2025. (received 04/02/2024)	
1.0	05/11/25	Dean Humphreys	Final revisions approved and updated to 1.0 for final release	