

Third-Party Vendor Management Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	4
4.1. Assigned Vendor Sponsor Responsibilities	4
5. Third Party Access Connections or Interfaces to OCA Systems.....	5
6. Vendor Register	5
7. Vendor Assurance Process	6
7.1. New or Changing Vendors	6
7.2. Existing Vendors	6
8. Third-Party Vendor Risk Assessment Process	7
8.1. Stage 1: Triage Risk Assessment.....	7
8.2. Stage 2: Vendor Self-Assessment.....	8
8.4. Stage 3: Remediation.....	9
9. Vendor Contracts	9
10. Vendor Management.....	9
11. Metrics and Reporting	9
12. Document Control	10
12.1 Document Revision History	10

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate information security requirements for vendor engagement, on-boarding and management.
- 1.2. The Open College of the Arts (OCA) engages and works with a number of third-party vendors. It is important that the security risks associated with working with vendors are identified and managed prior to any access to OCA's information and information systems. This policy sets out the requirements to ensure vendors collaborating with or providing products or services to the OCA, do so securely. It outlines the requirements and framework used to assess, manage and audit all vendors of technology or information related products and services.

2. Scope

- 2.1. This policy applies to:
 - All vendors that provide IT services or information security services to OCA;
 - All vendors that store, process or otherwise have access to Non-Public OCA information (of any type).
- 2.2. This policy is intended for the following OCA stakeholders:
 - IT Manager (Responsible for Information Security);
 - IT Department;
 - Finance Department;
 - All departments who carry out procurement processes.
- 2.3. **This policy shall not be provided to any vendor**, as this would pose a risk that they could undermine the assurance process or could gain an unfair commercial advantage over competitors that have not seen this policy.

3. Policy Statement

- 3.1. The policy of the OCA regarding vendor management is as follows:
 - Vendors shall be managed consistently and via a standardised process across the organisation from an information security point of view.
 - Unintended and unmanaged information security risks shall not be introduced as a result of vendor engagement and use.
 - Effective due diligence shall take place prior to agreeing terms with a vendor.
 - All agreements with vendors shall be managed by the organisation – a process coordinated by the assigned Vendor Sponsor.
 - All OCA data collected and handled by vendors shall be securely managed.

- Where OCA uses cloud services, responsibilities for cloud security shall generally be shared between cloud service providers (CSP) and OCA as cloud service customer (CSC), in line with the Shared Security Responsibility Model. The split of responsibilities shall be clearly documented in contractual terms.

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 Vendor Sponsor will comply with their specific responsibilities outlined in this policy.
- All OCA staff who engage with third party vendors, including the IT Department, Vendor Sponsors, Information Asset Owners and Business System Owners, shall comply with this policy.

4.1. Assigned Vendor Sponsor Responsibilities

- 4.1.1. All new, potential new and existing vendors shall have an assigned sponsor within OCA.
- 4.1.2. It is the responsibility of the assigned sponsor to:
 - Ensure that any third-party service which include a technology component (such as a website or application) must be registered with the college's central list of technology. The assigned sponsor must ensure that any third-party service which includes a technology component must plan for decommissioning at the end of life, or when the service is no longer required.
 - When engaging with a third party for the first time, a Non-Disclosure Agreement (NDA) must be signed before any OCA information is disclosed.
- 4.1.3. All third parties engaged to provide services to the OCA must have a contract in place. The contract must include the following:
 - Confidentiality clause.
 - Agreement to follow all OCA Information Security policies.
 - Requirements to keep any technology supported and patched for the duration of the contract.
 - Secure disposal of OCA information upon termination of contract.
- 4.1.4. Consult with the IT Services Team as early as possible in order to ensure that appropriate due diligence is undertaken.
- 4.1.5. The Vendor Sponsor is responsible for ensuring that; the appropriate agreements and contracts are in place; the third-party access rights to information and information systems are provisioned in accordance with the Information Asset Owner's approval and that where software development

is outsourced to a third party, requirements of the [Secure Software Development Policy](#) are implemented.

- 4.1.6. All contracts with third parties for the supply of services to the College will be monitored and reviewed to ensure that information security requirements are being satisfied.
- 4.1.7. Third parties must notify the OCA of any security incidents impacting OCA information or information systems within the terms specified in the Service Level agreement (SLA).

5. Third Party Access Connections or Interfaces to OCA Systems

- 5.1. All third-party connection requests must have approval from the following; Vendor Sponsor, Information Asset Owner, and IT Services before being granted.
- 5.2. Where third party access is granted, connectivity must be provisioned through approved OCA solutions, strictly restricted to only the resources and data required to carry out the work.
- 5.3. Third party connections must be terminated when no longer required and may be terminated in the event of a security breach.
- 5.4. The OCA will monitor third party connections for the detection and prevention of unauthorised access.
- 5.5. A central register of all third-party connections will be maintained by the IT Services team and will be reviewed and updated quarterly or as necessary.
- 5.6. Third party access to information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).
- 5.7. Third parties must agree to adhere to OCA Information Security and Data Protection Policies.

6. Vendor Register

- 6.1. OCA shall create and maintain a central vendor register that provides a record of all vendors and key attributes (e.g. vendor name, service description, contact details, vendor sponsor), as well as the level of security assurance that has taken place for each vendor.

7. Vendor Assurance Process

- 7.1. OCA shall have an established vendor assurance process (The [Third-Party Vendor Management Process](#)) that comprises several stages:

- A high-level triage risk assessment of a new vendor, done internally by OCA as part of the due diligence process before onboarding that vendor (Stage 1).
- Should the outcome of the triage risk assessment identify a vendor as Medium or High risk, a Third-party Vendor Information Security Questionnaire (self-assessment) will be issued (Stage 2).
- Depending on the outcome of the previous stage(s), a remediation stage (Stage 3).

7.2. The vendor assurance process shall also be applied to existing vendors in any of the following cases:

- When there is a significant change or extension of the services provided by the exiting vendor;
- When the contract with an existing vendor is reaching its end, and the vendor has not been subject to the vendor assurance process before.

7.3. In the case where a given vendor provides the same service to two or more departments of OCA, the vendor assurance process can be applied across the relevant business departments.

7.4. New or Changing Vendors

7.4.1. To ensure that the vendor assurance process is initiated in a timely fashion, the Vendor Sponsor must inform the IT Manager when:

- Engaging any potential new vendor, including as part of a tender evaluation process;
- There are changes to an existing vendor's services; or
- An existing vendor's contract is coming to an end.

7.4.2. It is then the responsibility of the IT Manager to carry out the risk assessment (Stage 1) of the vendor in collaboration with the Vendor Sponsor.

7.5. Existing Vendors

7.5.1. In order to ensure all active vendors or those who have an ongoing commercial or technical accountability or responsibility to OCA go through the vendor assurance process, there must be processes in place to review existing vendors. This will identify vendors that may have been onboarded prior to this policy being established. Those vendors who are no longer commercially or technically accountable or responsible to OCA shall be considered, where commercially and legally viable, for removal from OCA systems, and data associated with said vendors, considered for removal under the Data Retention and Disposal Policy.

- 7.5.2. To conduct this review, the IT Department is responsible for providing the IT Manager with a list of all existing vendors who meet the above requirements on an annual basis.
- 7.5.3. In order to ensure that vendor assurance for these vendors is adequately addressed, the IT Manager shall adopt a risk-based approach to prioritising vendors that have not gone through vendor due diligence.

8. Third-Party Vendor Risk Assessment Process

8.1. Stage 1: Triage Risk Assessment

- 8.1.1. A triage risk assessment shall be carried out on all vendors that could affect information security, irrespective of the value of the contract, to provide an inherent risk rating.
- 8.1.2. The Vendor Sponsor, in collaboration with the IT Department is responsible for carrying out this assessment.
- 8.1.3. The triage risk assessment must be aligned to the [Information Security Risk Management Policy](#) and include an assessment of:
 - The classification of data the vendor will process or have access to;
 - Where the vendor will access data from;
 - Where data will be stored by the vendor;
 - The level of access the vendor will have to the OCA systems;
 - The potential impact to the OCA, if the vendor suffered an information security incident;
 - The potential impact that a disruption to the vendor's service could have on the OCA's business objectives;
 - Where the vendor is providing services via a Cloud or Managed Service, assurances around the physical, logical and process controls for all Cloud or Managed Services and/or hosting providers used.
- 8.1.4. It is the responsibility of the IT Manager to review the completed risk assessment, decide whether further due diligence is required, and communicate their findings and recommendations to the Vendor Sponsor.
- 8.1.5. Where OCA obtains confirmation that a vendor is certified against relevant information security standard(s), this may be considered as sufficient assurance regarding the level of risk posed by using the vendor's services. In this case, pending the approval of the IT Manager, no further due diligence shall be required.

8.2. Stage 2: Vendor Self-Assessment

- 8.2.1. Following the triage risk assessment (Stage 1), all vendors that the IT Manager has assessed to represent a medium or high risk to OCA shall

undergo further due diligence. This involves the vendor answering a self-assessment questionnaire to evaluate its information security controls and maturity across the following areas:

- Information security governance and organisation;
- Certifications and standards alignment;
- Data transfer agreements in place and adherence to applicable local legislation;
- Policies and procedures;
- Information security risk management;
- Human resource security (including training and vetting of staff/contractors);
- Asset management;
- Access control;
- Physical security (including data centre security, if applicable);
- Operations security;
- Communications security;
- System acquisition, development and maintenance;
- Vendor relationships (if there is subcontracting) including any SLA dependencies;
- Change management;
- Business continuity;
- Information security incident response;
- Data loss prevention;
- Data privacy;
- Malware prevention;
- Security by design / coding standards adhered to;
- Service and support.

8.2.2. The Vendor Sponsor and the relevant procurement department are responsible for ensuring the vendor completes the self-assessment questionnaire. The IT Manager is then responsible for reviewing the responses that the vendor has provided, assessing the response to each control question and providing a list of perceived control gaps for the vendor (if any), alongside an overview of the level of residual risk that the vendor represents on the basis of the self-assessment.

8.3. Stage 3: Remediation

- 8.3.1. Where there are any shortfalls in expected vendor controls that have been identified as part of the stage 2 assessment, these must be followed up with the relevant teams. The Vendor Sponsor, the IT Department and other stakeholders must agree remediation requirements and delivery dates with the vendor; remediation requirements must be raised as risks and tracked via risk management processes, in line with the [Information Security Risk Management Policy](#).

9. Vendor Contracts

- 9.1. The Vendor Sponsor is responsible for engaging with the Legal Department and the IT Manager in drafting a contract which contains relevant clauses and also addresses any issues which may have been flagged through the vendor assurance work. The contract shall include a right of the OCA to audit the vendor and their operational / infrastructure environments. The contract shall also contain reference to relevant information security policies and requirements, including but not limited to:
- Non-Disclosure Agreements (NDAs);
 - Agreements on information security, information transfer and network and information access;
 - Shared responsibilities;
 - Agreements on remote working.

10. Vendor Management

- 10.1. Every vendor shall be reviewed on contract renewal, or sooner, if circumstances such as legislation, regulations, vendor disclosed incidents or contracts require it. This is to confirm that:
- No changes have occurred to the services being provided that may require the vendor to undergo another risk assessment;
 - OCA data and service availability are unaffected by any third-party activity or incident;
 - No changes to the control coverage of the vendor have occurred that may require the vendor to undergo another assessment.
- 10.2. When a vendor has been reviewed, the vendor register shall be updated accordingly.

11. Metrics and Reporting

- 11.1. Relevant metrics for vendor management shall be defined, and regularly obtained and reported to the OCA Board.
- 11.2. Analysis of metrics shall be used to assess the efficiency of the vendor management processes and continuously improve them.

12. Document Control

Document Control	
Title:	Third-Party Vendor Management Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

12.1 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