

Cryptographic Controls Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	4
5. Use of Encryption	4
6. Encryption Algorithms and Key Lengths	5
7. Key Management	5
8. Use of Digital Signatures and Certificates	7
9. Certificate Management	7
10. Legal and Regulatory Constraints	8
11. Changes of Cryptographic and Key Management Systems and Technologies	8
12. Cloud Services	8
13. Metrics and Reporting	8
14. Policy Review Date	8
15. Document Control	9
15.1 Document Revision History	9

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate the minimum requirements for use of cryptography in the protection of The Open College of the Arts (OCA) data. It is independent of any hardware and software environment and shall be used as a generic baseline for the implementation of cryptographic controls for any system or application.

2. Scope

- 2.1. This policy applies to the OCA's IT networks and systems.
- 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 cryptographic controls is as follows:

Cryptographic techniques shall be used:

- To protect 'Confidential' or 'Highly Confidential' information both in storage and when in transit;
- When information is at risk of disclosure or modification, or actions are at risk of repudiation (denial of the action), and existing controls do not reduce such risk to an acceptable level.
- Information that requires encryption shall be secured to approved standards and in line with the legal and regulatory requirements of the OCA.
- Information / data owners shall define the data needing encryption based on the [Information Classification and Handling Policy](#).
- Encryption strength shall have a minimum baseline strength, but shall be variable above this minimum standard, appropriate to the expected data value lifetime such that it could only be disclosed by brute-force or other methods after the data has lost its commercial value.
- Use of cryptography shall adhere to and follow all applicable laws and regulations regarding cryptographic controls.
- Data shall only be encrypted by approved and authorised cryptographic methods. These shall be based upon proven and publicly available algorithms in accordance with internationally recognised standards bodies¹.

¹ Such as: National Institute of Standards and Technology (NIST); International Organization for Standardization (ISO); Internet Engineering Task Force (IETF); American National Standards Institute (ANSI); and Institute of Electrical and Electronics Engineers (IEEE).

- Data taken outside of the OCA premises shall be protected using approved cryptography tools commensurate with sensitivity. This includes data on all mobile computing and storage devices and electronic media.
- An appropriate key management system shall be established and maintained to ensure confidentiality, integrity and availability of the keys throughout the key lifecycle.
- Public key certificates shall be used to verify ownership of public keys.

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 shall comply with this policy for all networks, applications and systems that it maintains. It shall also be responsible for:
 - Developing and implementing key and certificate management procedures in line with this policy;
 - Maintaining key and certificate inventories in line with this policy;
 - Defining the responsibilities for specific roles involved in key management activities, as applicable (key managers, key custodians and key witnesses).
- Business system owners shall comply with this policy for any information systems that they are responsible for managing.
- All the OCA staff have a responsibility to adhere to this policy.

5. Use of Encryption

5.1. The following encryption controls shall be applied:

- Stored information shall be encrypted when the information is classified as 'Confidential' or 'Highly Confidential', for third party storage and portable storage media in use.
- Transmitted information outside of the OCA Network shall be encrypted when the confidentiality of information is classified as 'Confidential' or 'Highly Confidential', regardless of the transmission mechanism in use.
- All mobile devices, e.g. laptops, mobile telephones, tablets and removable media such as Universal Serial Bus (USB) sticks, shall use encryption to protect data at rest.
- Devices used by homeworkers shall use encryption to protect data at rest and for connectivity to the OCA's networks and systems.
- All external remote access to the OCA's network shall use encryption, i.e. Virtual Private Network (VPN) technology.
- All the OCA wireless networks shall use encryption, using algorithms, protocols and configurations that are aligned to industry best practices.
- All network communication links over untrusted networks shall be encrypted.

- All authentication credentials shall be encrypted and all logon authentication using passwords shall use encrypted transmission links.
- All websites hosted by the OCA which are used for either transactional purposes or for the communication of sensitive information between the OCA and its customers, staff or students shall be encrypted using the most up to date version of digital certificates signed by an external certification authority.
- Backups shall be encrypted using at least the minimum approved levels of encryption, in line with the [Backup and Recovery Policy](#).
- Use of deprecated cryptographic protocols² shall be avoided.
- Risks associated with the use of encryption shall be assessed and managed, in line with the [Information Security Risk Management Policy](#).
- Encryption and key management systems, policies and processes shall be regularly audited, in line with the [Information Security Audit and Compliance Policy](#).
- Any migration of servers, services, applications or data to cloud environments shall be done using secure and encrypted communication channels.

6. Encryption Algorithms and Key Lengths

- The OCA shall only use encryption algorithms and key lengths that are recognised by the information security industry.
- Algorithms and key lengths shall be replaced as soon as it is recognised by the information security industry that they have become vulnerable to exploitation.
- An up-to-date list of acceptable algorithms and key lengths shall be documented.
- Key-encrypting keys shall be at least as strong as the data-encrypting keys that they protect. They shall also be stored separately from the data-encrypting keys.

7. Key Management

- 7.1. A formal management system for keys and other cryptographic materials shall be put in place to ensure that encrypted information is not compromised or lost in the event of keys or materials being lost, compromised, expired or damaged.
- All keys shall be protected against modification or destruction.
 - Secret and private keys shall be protected against unauthorised disclosure and stored in the fewest possible locations.
 - Systems used to generate, store, distribute and archive cryptographic keys shall be protected by adequate physical security.

² Like Secure Sockets Layer (SSL), or Transport Layer Security (TLS) versions earlier than 1.2.

- Cryptographic keys shall have defined validity dates in order to reduce the likelihood of compromise, e.g. after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key, as defined by the associated application vendor or key owner and based on industry best practices and guidelines.
- Public key certificates shall be used to verify ownership of public keys. The management process used to generate such certificates shall be trusted and may be carried out by an external Certification Authority (CA).
- Formal key management procedures and, where applicable, technical measures, shall exist³ for:
 - Generation of strong cryptographic keys;
 - Secure cryptographic key distribution;
 - Secure cryptographic key storage;
 - Deactivation of keys that have reached the end of their crypto period;
 - Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened, e.g. as a result of departure of an employee with knowledge of a clear-text key component, or because keys are suspected of being compromised, or because an entity is no longer part of the OCA⁴⁵;
 - Any manual clear-text cryptographic key-management operations in use, which shall be managed using split knowledge and dual control⁶;
 - Prevention of unauthorised substitution of cryptographic keys;
 - Creation of keys in a pre-activated state, but not authorised for use;
 - Key transitions from any state to/from suspension;
 - Management of archived keys in a secure repository requiring least privilege access;
 - Use of compromised keys to encrypt information only in controlled circumstances, and thereafter exclusively for decrypting data and never for encrypting data;
 - Assessment of the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost;
 - Formal acknowledgement by key managers, key custodians and key witnesses of their understanding and acceptance of their responsibilities.
- Key management activities shall generate audit trails with the relevant information.
- An inventory of keys shall be maintained and kept up to date.

³ Including, where applicable, provisions for legal and regulatory requirements.

⁴ If retired or replaced cryptographic keys need to be retained, these keys shall be securely archived, e.g. by using a key-encryption key. Archived cryptographic keys shall only be used for decryption/verification purposes.

⁵ Including, if applicable, keys stored in Hardware Security Modules (HSMs).

⁶ Examples of manual key-management operations include, but are not limited to key generation, transmission, loading, storage and destruction.

- Access to keys shall be restricted to the fewest number of people and only when genuinely required.
- When keys are password protected, the password formatting and length shall be in line with the requirements for IT administrator passwords, as documented in the [Access Control Policy](#).
- For wireless environments connected to systems where Confidential or Highly Confidential data is stored or transmitted, wireless encryption keys shall be changed when any of the following applies:
 - Personnel with knowledge of the key leave the OCA or the role for which the knowledge was necessary;
 - A key is suspected of or known to be compromised.

8. Use of Digital Signatures and Certificates

8.1. Digital signatures and certificates shall be employed where required to:

- Protect and verify the authenticity and integrity of electronic documents which are classified as 'Confidential' or 'Highly Confidential', or are involved in critical transactions;
- Establish a relationship of authentication and trust between entities or individuals;
- Demonstrate non-repudiation of messages or transactions.

8.2. Where digital signatures are used for authentication, the following shall apply:

- Digital signatures shall be created using the OCA approved electronic signature technologies. They shall be:
 - Unique to the person using it;
 - Capable of reliable verification; and
 - Linked to specific data so that if the data is changed the electronic signature is invalidated;
- Keys used for digital signatures, digital certificates and user authentication shall never be included in a key escrow arrangement;
- Under no circumstances shall keys that are used to create digital signatures, digital certificates or user authentication be backed up outside of the OCA approved processes;
- If a digital signature is compromised, it shall immediately be reported as an information security incident and responded to in line with the [Information Security Incident Response Policy](#). In addition, the users of digital signatures whose certificates have been lost or compromised shall immediately notify the originator of the data.

9. Certificate Management

- 9.1. A system for the management of public key certificates shall be established. The system shall ensure that:
- All certificates are signed by a CA;
 - An inventory of all key certificates in use (including root certificates) is maintained;
 - Where a root certificate is due to expire within 12 months, plans will be put in place to ensure a smooth migration to a new CA and rekeying or replacement of keys whose trust is reliant on the previous CA;
 - The integrity and availability of certificates is monitored.

10. Legal and Regulatory Constraints

- 10.1. The appropriate legal and regulatory frameworks shall be taken into account when considering the deployment of cryptographic controls, particularly with transnational exchanges of information. Certain countries prohibit encryption technologies or strongly regulate the types of permissible cipher.
- 10.2. Relevant advice shall be sought from the Legal Department.

11. Changes of Cryptographic and Key Management Systems and Technologies

- 11.1. Any changes to cryptographic or key management systems or technologies used by the OCA shall be subject to established change management procedures, in line with the [Change Management Policy](#).

12. Cloud Services

- 12.1. Where the OCA uses cloud services, the responsibilities for cryptographic controls can be shared between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC), in line with the Shared Security Responsibility Model.

In all cases, the split of responsibilities shall be clearly documented in contractual terms.

13. Metrics and Reporting

- 13.1. Relevant metrics for the use of cryptography shall be defined, and regularly obtained and reported to the Finance, Employment, Audit and Risk (FEAR) Committee and The OCA Board as appropriate.
- 13.2. Analysis of metrics shall be used to assess the efficiency of the cryptographic controls and to continuously improve them.

14. Policy Review Date

- 14.1. 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.

15. Document Control

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

15.1 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