

Information Classification & Handling Policy

Table of Contents

1.	Purpose	3
2.	Scope	3
3.	Introduction to the Policy	3
4.	Policy Statement.....	3
5.	Roles and Responsibilities.....	4
6.	Information Classification Categories	4
7.	Access to Information	5
8.	Information Ownership	5
9.	Classification of Information.....	6
9.1	Generalities	6
9.2	Classifying Public Information	6
9.3	Classifying Non-Public Information.....	6
9.4	The Principle of Aggregation	6
9.5	Changes to Classification	7
10.	Marking of Information	7
10.1	Generalities	7
10.2	Visibility of Marking.....	7
10.3	Other Markings.....	7
11.	Transmission of Information	8
11.1	Generalities	8
11.2	E-mail and Electronic Transmission	8
11.3	Transmission by Physical Delivery	9
11.4	Voice Transmission	9
11.5	Printing	10
11.6	Publication or Display of Information	10
12.	Storage of Information	10
13.	Disposal of Information.....	11
13.1	Disposal of Electronic Information	11
13.2	Disposal of Printed Information	11
14.	Data Inventory	11
15.	Incident Management	11
16.	Policy Review Date.....	12
17.	Appendix A – Information Classification and Handling Matrix.....	13
18.	Document Control.....	17
18.1	Document Revision History	17

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate The Open College of the Arts (OCA)'s policy in regard to the classification and handling of information. More specifically, it is to ensure that all the OCA information:
- Is classified in a standard, consistent manner, linked to the consequences of its unauthorised disclosure, modification or loss;
 - Is handled with an appropriate level of protection, in line with its classification.

2. Scope

- 2.1. This policy applies to all the OCA information, in digital or printed form, structured or unstructured, and including, where applicable, information of external origin that comes under the control of the OCA.

3. Introduction to the Policy

- 3.1. Information is a valuable OCA asset embodying varying degrees of confidentiality and criticality. The OCA's information classification system described within this policy is used to categorise information based on an assessment of the impact if the information were to be lost, corrupted or disclosed to an unauthorised person. This ensures that the information receives the appropriate level of protection.
- 3.2. Classifications and associated protective controls take account of business needs and the requirements for sharing or restricting information. The classification given to information is therefore a shorthand way of communicating how it is to be handled and protected.

4. Policy Statement

- 4.1. The policy of the OCA in regard to information classification and handling is as follows:
- All the OCA information shall be categorised and allocated a standard classification based on the consequences of its unauthorised disclosure, modification or loss.
 - All the OCA information shall be handled and protected at a minimum in accordance with the requirements for its classification.

5. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- Information owners¹ are primarily responsible for the classification and marking of the information that they own. (See sections 9 and 10 below for details.)
- The IT Team in consultation with the Data Protection Officer (DPO) are responsible for ensuring that the requirements for classification and handling of personal data are compliant with the applicable data protection regulations.
- All staff and relevant third parties have a responsibility to protect information by handling it in line with this policy.

6. Information Classification Categories

- 6.1. All the OCA information shall be categorised with a classification.
- 6.2. The OCA information falls into four categories, Public, Internal, Confidential and Highly Confidential, as described below:
 - **Public:**
 - Information in the public domain, the unauthorised disclosure, modification or loss of which would **cause no damage to the OCA, its employees and/or partners.**
 - **Internal:**
 - Information of a moderate degree of sensitivity, the unauthorised disclosure, modification or loss of which would **be detrimental to the interests of the OCA, its employees and/or partners.**
 - **Confidential:**
 - Information of a high degree of sensitivity, the unauthorised disclosure, modification or loss of which would **likely cause significant harm to the interests of the OCA, its employees and/or partners.**
 - **Highly Confidential:**
 - Information of the highest degree of sensitivity, the unauthorised disclosure, modification or loss of which would **cause very significant harm to the interests of the OCA, its employees and/or partners.**

¹ These responsibilities can be delegated.

- 6.3. In this policy and other the OCA documentation, the term Non-Public² will be used to refer collectively to information that is not Public – i.e., that is either Internal, Confidential or Highly Confidential.
- 6.4. The sections that follow prescribe the requirements for the handling of information according to its classification. These requirements, as well as examples of the different types of information within each category, are summarised in **Appendix A - Information Classification and Handling Matrix**.

7. Access to Information

- 7.1. Access to all Non-Public information shall be granted on the principle of personnel being given the minimum access needed to perform their role. This means that access to any Non-Public information shall be denied unless it is specifically required.
- 7.2. Access to Confidential and Highly Confidential information shall be restricted to:
- Permanent the OCA employees who have signed an OCA employment contract incorporating standard confidentiality provisions, or a confidentiality or non-disclosure agreement;
 - Contractors, temporary staff, and other third parties who have signed a confidentiality or non-disclosure agreement with the OCA.

8. Information Ownership

- 8.1. The information owner is the formal owner of an information asset and is accountable for protection of the information. The information owner can be a specific role or department that is responsible for managing the lifecycle of the information. Information owners shall be identified in the relevant information asset inventories, which shall be reviewed at least annually, in line with the Asset Management Policy.
- 8.2. Information owners are typically directors, managers or programme leaders; however, in practice, information owner responsibilities can be, and often are, delegated to technical system/service owners or supplier managers that, as information stewards, are responsible for the day-to-day operational management of the system/service.
- 8.3. Where the information owner is not explicitly stated or registered, then the information owner is, by default, the person that created the document or the person responsible for the system or process that captured the information.

² The term 'sensitive', which can at times be found with the same meaning in documentation, shall generally be avoided in this sense, as it is often used with a more specific meaning in other contexts (e.g. 'sensitive personal data' referring to 'special categories of data') and could lead to ambiguity.

9. Classification of Information

9.1. Generalities

- 9.1.1. The information owners have the primary responsibility for classifying the information owned by them.
- 9.1.2. In addition to the requirements for marking of classification (see section 10 below), the classification of information shall also be reflected in the relevant information asset inventories. Where information resides in a system or database, the relevant associated documentation shall also indicate the classification of the information that resides in it.
- 9.1.3. Information is classified to indicate whether protection is needed, protection priorities and the degree of the protection. Therefore, it is important not to over-classify - this not only avoids unnecessary business restrictions but also prevents strain on the security mechanisms and degradation of the protection of more sensitive items.

9.2. Classifying Public Information

- 9.2.1. All Public information shall be classified as such when:

- Public information is created either in electronic or in printed form;
- Information received from third parties is identified as containing no confidential information nor requiring any special handling.

9.3. Classifying Non-Public Information

- 9.3.1. All Non-Public information shall be classified as Internal, Confidential or Highly Confidential when:

- Non-Public information is created either in electronic or in printed form;
- Information received from third parties is identified as containing confidential information, or as otherwise requiring special handling. Care shall be taken when interpreting classification labels appearing on information received from other organisations, as the labels they use may be different to those adopted by OCA.

9.4. The Principle of Aggregation

- 9.4.1. Whilst one piece of information may be classified at a particular level, a set of similar pieces of information held together may be classified at a higher level. When dealing with aggregated information, the information owner shall identify the classification for the aggregated set of information, and the information set shall be treated at that classification level whilst it is held as an information set.

9.5. Changes to Classification

- 9.5.1. The classification level of any item of OCA information can be upgraded (for example, changed from Internal to Confidential) when information has been identified as requiring a more restricted classification. However, only the information owner can 'declassify' or downgrade the classification level (for example, change the classification level from Internal to Public).

10. Marking of Information

10.1. Generalities

- 10.1.1. The information owners have the primary responsibility for marking the information owned by them, in accordance with its classification.
- 10.1.2. Internal, Confidential and Highly Confidential information shall be marked as 'Internal', 'Confidential' and 'Highly Confidential', respectively. In the case of documents, this shall be done within the documents themselves. In the case of information that resides in a system or database, the relevant associated documentation shall also indicate the classification of the information that resides in it.
- 10.1.3. Where feasible, automated marking processes shall be established, e.g. to facilitate the marking of e-mails and business documents.
- 10.1.4. All OCA personnel who have access to Non-Public information shall understand how to classify, mark and handle information. In case of doubt, contact the IT Department.

10.2. Visibility of Marking

- 10.2.1. Non-Public information shall be clearly marked so that its classification is immediately identifiable by anyone handling the information. Documents (of any type; including not only text documents but also spreadsheets, presentations, etc.) shall have the classification in the header or footer of each page/tab/slide, or in an equally visible location, depending on the type of document. Similarly, e-mails shall have the classification either in the subject line or at the beginning of the text in the body of the e-mail.

10.3. Other Markings

- 10.3.1. In addition to the marking requirements of OCA information contained in this policy, OCA shall also comply with any other marking standards that may be required by local law, regulation and contractual obligations. Such additional markings shall be included in addition to the information markings required by this policy.

11. Transmission of Information

11.1. Generalities

- 11.1.1. When Non-Public information is to be transmitted electronically, or delivered physically, either within the company or externally, the classification shall be taken into account.

- 11.1.2. Non-Public information shall only to be transmitted to individuals or organisations authorised to receive such information, and then only to the extent the recipient needs to know such information. The sender of such information is responsible for ensuring that the recipients are authorised, prior to sending. Confidential and Highly Confidential information shall only be transmitted to authorised individuals or organisations who have signed a confidentiality or non-disclosure agreement with the OCA.
- 11.1.3. There shall be agreements in place to address the secure transfer of Non-Public information between the OCA and external parties.
- 11.1.4. The subsections that follow describe the constraints applicable to the transmission of information using specific channels and technologies. The [Acceptable Use Policy](#), and other policies referenced in some of the subsections, contain more information about the use of such channels and technologies.

11.2. E-mail and Electronic Transmission

- 11.2.1. Non-Public information in electronic form shall only be transmitted using IT approved file-sharing systems (e.g. Google Drive, MS OneDrive and Sharepoint) and facilities with appropriate access restrictions applied.
- 11.2.2. Confidential and Highly Confidential information shall be encrypted in transit – see the [Cryptographic Controls Policy](#) for details. (If in doubt, contact the IT Department.)
- 11.2.3. When transmission of Confidential or Highly Confidential information by e-mail is required, Gmail's 'Confidential Mode' should be used where appropriate and practical.
- 11.2.4. See the [Online Behaviour and Social Media Policy](#) for more information on the use of e-mail.
- 11.2.5. Mobile messaging applications and SMS are common mediums for the exchange of information but pose risks to the security of the information.
- 11.2.6. Internal and Confidential information shall not be sent by mobile messaging applications or SMS unless explicitly authorised by the IT Department.
- 11.2.7. Highly Confidential information shall not be sent by mobile messaging applications or SMS in any circumstances.

11.3. Transmission by Physical Delivery

- 11.3.1. When being delivered physically, the OCA information shall be packaged and delivered according to its classification.
- 11.3.2. Internal information shall be delivered by hand if possible. For internal delivery, an internal mail envelope shall be used. For external delivery, a sealed envelope shall be used.
- 11.3.3. Confidential information shall be delivered by hand or sent by registered mail or trusted courier; receipt shall be confirmed. For

internal delivery, a sealed envelope inside an internal mail envelope shall be used. For external delivery, a sealed envelope marked 'Confidential' shall be put inside a mail envelope addressed to a specific person, with no outer markings indicating that Confidential documents are contained therein.

- 11.3.4. Highly Confidential information shall be delivered by hand or sent by trusted courier; receipt shall be confirmed. For internal delivery, a sealed envelope inside an internal mail envelope shall be used. For external delivery, a sealed envelope marked 'Highly Confidential' shall be put inside a mail envelope addressed to a specific person, with no outer markings indicating that Highly Confidential documents are contained therein.

11.4. Voice Transmission

- 11.4.1. Phone calls are inherently insecure. Non-Public information shall not be discussed on the phone or similar voice technologies unless all of the following apply:
- The identity of the person being spoken to is known;
 - There is a business requirement for the person to receive information by voice technology;
 - Steps are taken to ensure that the conversations cannot be overheard.
- 11.4.2. Additionally, where there is a business need to share Confidential or Highly Confidential information on voice technologies, it must be ensured that the identity of the person(s) being spoken to is verified³.
- 11.4.3. The discussion of Internal information in public areas shall be avoided if possible, and, where taking place, steps shall be taken to prevent eavesdropping.
- 11.4.4. Confidential and Highly Confidential information shall not be discussed in public areas in any circumstances.

11.5. Printing

- 11.5.1. Where printed on OCA equipment, Non-Public information shall be collected immediately from the printer and stored in accordance with its classification. Whenever possible, 'Follow Me Printing' shall be used.
- 11.5.2. Printing of Internal or Confidential information on non-the OCA equipment shall be avoided, as a printer may retain copies of documents within its memory – unless steps are taken to ensure that such copies are effectively deleted.
- 11.5.3. Highly Confidential information shall not be printed on non-OCA equipment in any circumstances.

³ Especially in the case where Highly Confidential information is transmitted, verification should not rely excessively on perceived voice recognition of known individuals. Use of video-conferencing should also be considered whenever feasible.

11.6. Publication or Display of Information

- 11.6.1. When information is to be published electronically or physically, either within the OCA or externally, its classification shall be taken into account.
- 11.6.2. Non-Public information shall not be displayed publicly either on external websites or in areas to which the general public have access.
- 11.6.3. Confidential and Highly Confidential information shall only be viewed on screen where there is no chance of unauthorised visibility of the information.

12. Storage of Information

- 12.1. Non-Public information in electronic format shall only be stored within IT approved systems and facilities, with strict access controls, logging and monitoring, in line with the [Access Control Policy](#) and the [Logging and Monitoring Policy](#).
- 12.2. Confidential and Highly Confidential information shall be encrypted at rest – see the [Cryptographic Controls Policy](#) for details.
- 12.3. Internal information in paper format shall be kept in locked cabinets outside of office hours.
- 12.4. Confidential and Highly Confidential information in paper format shall be kept in locked cabinets accessible only to authorised individuals, outside of office hours and whenever left unattended.
- 12.5. Storage of Non-Public information in third party facilities/systems shall only occur with explicitly approved third parties that have gone through supplier due diligence, in line with the [Third-Party Vendor Management Policy](#)

13. Disposal of Information

13.1. Disposal of Electronic Information

- 13.1.1. Simply selecting 'delete' on documents within a file share or 'emptying the recycle bin' does not render the data unrecoverable and these methods shall not be used as a means of ensuring electronic information has been disposed of.
- 13.1.2. The deletion of Non-Public information from computers or electronic media shall be done using secure deletion guidelines provided by the IT Department. (If in doubt, contact the IT Department.)
- 13.1.3. When equipment containing Non-Public information is redeployed or disposed of, the information held on it shall be securely deleted. Under all circumstances, this will be undertaken by the IT Department.
- 13.1.4. See the [Data Retention and Disposal Policy](#) for more information on disposal of electronic information.

13.2. Disposal of Printed Information

- 13.2.1. When an item of printed Non-Public information is to be disposed of, it shall either be shredded or disposed of in a secure confidential waste

bin. In the case of Confidential or Highly Confidential information, a cross-cut shredder shall be used.

- 13.2.2. See the [Data Retention and Disposal Policy](#) for more information on disposal of printed information.

14. Data Inventory

- 14.1. The OCA shall create and maintain – at least for data classified as Confidential or Highly Confidential – a data inventory, identifying the type, location (including storage / processing / backup locations), volume and context of data. The IT Manager shall be responsible for keeping the data inventory up to date, with support from information owners.
- 14.2. Data discovery activities shall be undertaken as required to enable the identification and inventory of the data, supported by automated tools, where possible.
- 14.3. The data inventory shall be reviewed at least annually.

15. Incident Management

- 15.1. If Non-Public information is lost or compromised or suspected of being lost or compromised, it shall be immediately reported to the Service Desk, in line with the [Information Security Incident Response Policy](#).

16. Policy Review Date

- 16.1. 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



The Open College of the Arts



The Open
University

17. Appendix A – Information Classification and Handling Matrix

CATEGORY	DEFINITION / RESTRICTIONS	EXAMPLES	MARKING	TRANSMISSION	STORAGE	DISPOSAL
PUBLIC	Information in the public domain, the unauthorised disclosure, modification or loss of which would cause no damage to the OCA. Information can be disclosed without restriction.	• Marketing materials such as advertisements, brochures, catalogues; • Published annual accounts; • Internet Web pages; • External recruitment notices. Open Educational Resources • Open access research information and publications; • College statistics and course information intended for public consumption	None.	No restriction. On OCA Network: Encryption not required Public Network: Encryption not required	No restriction. On OCA network: Encryption not required Third party storage: Encryption not required Portable devices and storage media: Permitted without encryption	Normal waste disposal.

CATEGORY	DEFINITION / RESTRICTIONS	EXAMPLES	MARKING	TRANSMISSION	STORAGE	DISPOSAL
INTERNAL	Information of a moderate degree of sensitivity, the unauthorised disclosure, modification or loss of which would be detrimental to the interests of the OCA. Information shall be controlled.	Data that is of a general business nature and is typically produced in day-to-day business operations. Most corporate information falls into this category: • Operating procedures; • Policies; • Service Level Agreements; • Internal vacancy notices; • Intranet Web pages. • Meeting and committee minutes. • Team and department specific documentation. • Anonymised student information. • Copyright protected educational and promotional resources.	'Internal' at the footer of each page. For information in databases/systems, marking shall be done in the relevant associated documentation / information asset inventories.	Must not be publicly displayed. Internally: no restriction. Externally: only to authorised third parties. Avoid discussion on phone; ensure no overhearing. Avoid discussion in public areas; ensure no eavesdropping. Collect printed information immediately. Avoid printing on non-the OCA equipment. Electronic: IT approved file-sharing systems/facilities. Do not send by SMS/mobile messaging unless authorised. On OCA Network: Encryption not required Public Network: Encryption not required Paper: Deliver by hand if possible. Internally: use an internal mail envelope. Externally: use a sealed envelope.	Storage in third party facilities/systems: only with explicitly approved third parties that have gone through supplier due diligence. Electronic: IT approved systems/facilities, with strict access controls, logging and monitoring. On OCA network: Encryption not required Third party storage: Encryption not required Portable devices and storage media: Permitted without encryption Paper: Store in locked cabinets out of business hours.	Electronic: Secure deletion guidelines provided by IT. Equipment redeployment or disposal by IT only and in accordance with the <u>Asset Management Policy</u>. Paper: Dispose using secure confidential waste bins or, if none are available, shred using an approved shredder.

CATEGORY	DEFINITION / RESTRICTIONS	EXAMPLES	MARKING	TRANSMISSION	STORAGE	DISPOSAL
CONFIDENTIAL	Information of a high degree of sensitivity, the unauthorised disclosure, modification or loss of which would likely cause significant harm to the interests of the OCA. Information shall be strictly controlled.	- Personal data (but not including 'special categories of personal data'); - Purchasing deals and arrangements, contracts and other commercial and legal documentation; - Authentication data such as PINS, passwords, VPN tokens; - Designs and details of mission critical systems and products.	'Confidential' at the footer of each page. For information in databases/systems, marking shall be done in the relevant associated documentation / information asset inventories.	Must not be publicly displayed. Internally: only to authorised staff. Externally: only to authorised third parties and subject to confidentiality agreement. Avoid discussion on phone; verify identities; ensure no overhearing. Do not discuss in public areas. Collect printed information immediately. Avoid printing on non-the OCA equipment. Electronic: Encryption shall be used. Use secure e-mail software if available. Do not send by SMS/mobile messaging unless authorised. On OCA Network: Encryption not required Public Network: Encryption required Paper: Deliver by hand or send by registered mail or trusted courier; receipt shall be confirmed. Internally: use a sealed envelope inside an internal mail envelope. Externally: Use a sealed envelope marked 'Confidential' inside a mail envelope addressed to a specific person, with no outer markings indicating that Confidential documents are contained therein.	Storage in third party facilities/systems: only with explicitly approved third parties that have gone through supplier due diligence. Electronic: IT approved systems/facilities, with strict access controls, logging and monitoring; encryption shall be used. On OCA network: Encryption not required Third party storage: Encryption required Portable devices and storage media: Permitted with encryption for approved devices Paper: Store in locked cabinets out of business hours or when unattended.	Electronic: Secure deletion guidelines provided by IT. Equipment redeployment or disposal by IT only and in accordance with the Asset Management Policy. Paper: Dispose using secure confidential waste bins or, if none are available, shred using an approved cross-cut shredder.

CATEGORY	DEFINITION / RESTRICTIONS	EXAMPLES	MARKING	TRANSMISSION	STORAGE	DISPOSAL
HIGHLY CONFIDENTIAL	Information of the highest degree of sensitivity, the unauthorised disclosure, modification or loss of which would cause very significant harm to the interests of the OCA. Information shall be strictly controlled on a need-to-know basis only.	• Company strategy or planning information; • Legally privileged information; • Special categories of personal data, i.e.: • Race; • Ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Trade union membership; • Genetic data; • Biometric data (where used for identification); • Health data; • Sex life; • Sexual orientation; • Bank account details; • Cardholder data.	'Highly Confidential' at the footer of each page. For information in databases/systems, marking shall be done in the relevant associated documentation / information asset inventories.	Must not be publicly displayed. Internally: only to authorised staff. Externally: only to authorised third parties and subject to confidentiality agreement. Avoid discussion on phone; thoroughly verify identities; ensure no overhearing. Do not discuss in public areas. Collect printed information immediately. Do not print on non-the OCA equipment. Electronic: Encryption shall be used. Use secure e-mail software if available. Do not send by SMS/mobile messaging. On OCA Network: Encryption not required Public Network: Encryption required Paper: Deliver by hand or send by trusted courier; receipt shall be confirmed. Internally: use a sealed envelope inside an internal mail envelope. Externally: Use a sealed envelope marked 'Highly Confidential' inside a mail envelope addressed to a specific person, with no outer markings indicating that Highly Confidential documents are contained therein.	Storage in third party facilities/systems: only with explicitly approved third parties that have gone through supplier due diligence. Electronic: IT approved systems/facilities, with strict access controls, logging and monitoring; encryption shall be used. On OCA network: Encryption not required Third party storage: Encryption required Portable devices and storage media: Permitted with encryption for approved devices only, with restrictions Paper: Store in locked cabinets out of business hours or when unattended.	Electronic: Secure deletion guidelines provided by IT. Equipment redeployment or disposal by IT only and in accordance with the Asset Management Policy. Paper: Dispose using secure confidential waste bins or, if none are available, shred using an approved cross-cut shredder.

18. Document Control

Document Control	
Title:	Information Classification & Handling Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

18.1 Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	Dean Humphreys		Final release draft updated for release