RECORDS MANAGEMENT POLICY

Contents

Document Control Information	
Version control	[v.3]
Owned by:	[Information Compliance Manager]
Latest amendment on:	[8 July 2022]
Approved by:	[Senior Leadership Team]
Approved on:	[12 July 2022]
Coming into effect on:	[12 July 2022]
Review date:	[July 2023]

1. Introduction

1.1. The University recognises that the efficient management of its records is necessary, to support its core functions, to comply with legal and regulatory obligations and to contribute to the effective overall management of the institution. This document provides the policy framework through which this

effective management can be achieved.

1.2. This policy sets out principles for ensuring that the University implements effective records management, and provides guidance on the retention and disposal of records.

2. Scope of the policy

2.1. This policy applies to all records created, received or maintained by staff of the institution in the course of carrying out their corporate functions, and addresses the requirements of the Lord Chancellor's Code of Practice on the Management of Records (issued under Section 46 of the Freedom of Information Act 2000). Records and documentation created in the course of research, whether internally or externally- funded are also subject to contractual record-keeping requirements.

2.2. Records are defined as all those documents, which facilitate the business carried out by the University and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

2.3. Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including process for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

2.4. A percentage of the university's records will be selected for permanent preservation as part of the institution's archives, for historical research and as an enduring record of the conduct of business.

3. Objectives

i) To effectively manage records, which represent a key asset to the University. The University Records Management Policy has the following specific objectives:

ii) To instil good practice in records management across the University.

iii) To ensure information can be retrieved quickly and efficiently.

iv) To provide a basis for a university-wide record-keeping program to manage records from their initial stages to record destruction or permanent retention as set out in the Records Retention Schedule.

v) To ensure that the University's record-keeping practices comply with the legislative requirements of both the Data Protection and Freedom of Information Acts.

vi) To ensure that electronic records are managed as part of a comprehensive record keeping program.

vii) To inform University staff of their record-keeping responsibilities in order that records are managed as a unified corporate resource.

4. Legislation and Compliance framework

4.1. The management of records held by the university is regulated by the following legislation:

i) UK GDPR and Data Protection Act 2018

ii) Freedom of Information Act 2000

iii) Limitation Act 1980

4.2. The Data Protection and Freedom of Information Acts contain provisions relating to the destruction or alteration of information or records after a legal access request has been received. Such destruction or alteration can be considered a disciplinary offence. The Freedom of Information Act 2000 also creates a criminal offence in relation to these actions.

5. Responsibilities

5.1. The University has a corporate responsibility to maintain its records and record- keeping systems in accordance with the regulatory environment. All staff employed by the University are responsible for the proper management of the records they create and use. They must ensure that records for which they are particularly responsible are accurate and are maintained and disposed of in accordance with the Records Retention Schedule. The Information Compliance Manager is responsible for the

development and general oversight of Records Management throughout London Metropolitan University.

5.2. Responsibility for the management of files created in each department and/or school should, ideally, be allocated to an individual in each department and/or school. The designated individual should also liaise with the Information Compliance Manager concerning all aspects of Records Management.

6. Relationship with existing policies

6.1. This policy has been formulated within the context of the University's Information Management Framework.

7. Management of records

7.1. The Information Compliance Manager in liaison with the COO, will promote and assist with the implementation of this policy. This will include:

    i) Ad hoc support, advice and guidance tailored to individual needs

    ii) Development of guidelines to show staff how to archive records, retrieve archived records and how to confidentially dispose of records

    iii) Monitoring compliance with this policy

8. Retention

8.1. Records retention is governed by the [Records Retention Schedule](). Retention periods are determined in accordance with legal and regulatory requirements, and to meet business needs by

    i) Retaining information about decision-making, to inform future decisions and activities.

    ii) Retaining evidence of activities to support accountability.

    iii) Scheduling destruction of records which are no longer needed.

8.2. Records should not normally be retained beyond their retention period. Some records which have passed their retention date will be reviewed for

archival value. Those physical records selected for preservation as archives are transferred to Special Collections.

9. Disposal

9.1.   Paper records should be destroyed by shredding and confidential shredding, in accordance with BS EN 15713. Electronic records should be destroyed by mechanisms which guarantee irretrievability: deletion is not destruction. Effective mechanisms include degaussing, electronic file shredding, reformatting and physical destruction of storage media.

9.2.   All copies of expired records should be destroyed, wherever they are held. Destruction should also be documented, to provide evidence that retention schedules have been followed and to prevent searching for material that no longer exists.

9.3.   All disposal of IT equipment must be conducted via ITS to ensure that it is done securely and that any information remaining on any storage device is securely wiped.