Records Management Policy

Contents

OVERVIEW AND PURPOSE

1. The purpose of this policy is to ensure the University maintains accurate, reliable and accessible records of its business activities, retained for as long as necessary and destroyed or archived in a timely manner.
2. Good practice records management enables the University to minimise risks and costs associated with data volumes, compliance and sustainability.
3. The policy aims to provide guidance for anyone concerned with the management of University records.
4. For the purpose of this policy, a record can be defined as “information created, received and maintained as evidence of a decision and as an asset by the University, in pursuit of legal or regulatory obligations, or in the transaction of business” (ISO15489).
5. Records may be legal records (e.g. a contract), transactional records (e.g. an approval) or knowledge records (e.g. statistical reports).
6. Examples of records include; committee agendas, papers, minutes and actions, financial reports, staff and student records. Emails and other messaging types are only considered to be records if they show evidence of a business decision.
7. Note that a record is not the same as other forms of information. Individuals will create and manage the processing of information that has many purposes, including for business personal, operational, administrative or other reasons.
8. Information not explicitly classified as records must still recognise the need to be compliant with legal, regulatory or other policy requirements, including financial, data protection, FOI and other regulations.
9. Responsibility for ensuring compliance remains with individual Information Asset Owners.
10. The table below shows some of the types of information held by the University:

Type	Examples
Records	Committee agendas, papers, minutes and actions, financial reports, staff and student records, policies and regulations
Other documents	Informal meeting notes, draft versions, individual task guides.
Transient messages	Emails, Teams chats, SMS, WhatsApp messages and any other messaging service content that does not meet the definition of a record or document.

SCOPE

11. The policy applies to information in any format, structured or unstructured, virtual or physical, onsite or offsite location.

12. The policy applies to all staff and affiliates, including contractors, temporary staff, student workers, collaborative partners and any third party in a contractual relationship with the University for the processing of data.

13. Information relating to externally funded research projects is included within the scope of this policy.

POLICY

RESPONSIBILITIES

14. The Compliance and Information Governance team (CIG) is responsible for provision of policy, training and awareness, and online guidance for staff and affiliates involved in the creation, processing and destruction or archiving of University records.

15. The CIG team will periodically audit records management practices around the University to monitor compliance with this policy.

16. The Information Technology Services team (ITS) is responsible for the provision of information management systems with records management functionality to support staff and affiliates in their responsibilities.

17. The ITS team is responsible for ensuring appropriate security measures are in place to meet the information security principles of confidentiality, integrity and availability.

18. The Collections team in the University's Library Services is responsible for arrangements to maintain archives and collections of special significance to the University.

19. Heads of Functions and Departments are Records Owners, accountable for records within their area. They are the information risk owner for their area, responsible for managing and resolving risks. They are also responsible for determining and establishing record controls and standards, and for training, monitoring and managing their staff in records management.

20. All staff and affiliates are responsible for maintaining accurate records of business decision making. Staff and affiliates are also responsible for ensuring all information is retained and destroyed or archived in compliance with legal, regulatory and retention policy requirements.

21. The Information Governance Committee (IGC) is responsible for review and approval of all information governance related polices, including this Records Management Policy.

APPROACH

22. The University Records Retention Schedule details retention periods for different types of information.

23. The Document Management Catalogue details default retention and deletion periods for information across the University's digital storage and collaboration services.

24. All information is deleted in accordance with the Records Retention Schedule and Document Management Policy to minimise compliance risks and storage costs, and to support the University's sustainability aims.

RELATED LEGISLATION, REGULATIONS AND POLICIES

25. Related legislation

- UK Data Protection Act 2018
- UK General Data Protection Regulation
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Limitation Act 1980

26. This policy should be read in conjunction with other relevant University policies and documents which can be viewed in the Information regulations section of the University website.

BREACH OF POLICY

27. Anybody handling data agrees to abide by the terms of any applicable policies. Users who are found to have breached the terms of relevant policies may be subject to warnings, verbal and written. In serious cases individuals will -be subject to the University's disciplinary procedures, or possible legal action.