Kingston University London

# Retention Policy

## Contents

## OVERVIEW AND PURPOSE

1. Data, information and records (hereafter information) are essential for enabling Kingston University to operate. This includes information relating to students and their study as well as the planning and running of the organisation. In general, information should only be kept for as long as is necessary to:
    - Provide a record of students' academic achievement
    - Support academic teaching, research and support services
    - Meet contractual obligations relating to staff, students and third parties
    - Ensure the effective running of university services and corporate administration
    - Ensure compliance with applicable legislation, regulatory requirements and audit requirements
    - Ensure compliance with the requirements of professional bodies and research funding bodies.
2. To support these purposes, information must be managed throughout its lifecycle of collection, processing, use, disclosure, retention and destruction.
3. The purpose of this policy and the related Records Retention Schedule are to provide a framework for the management of the university's information through its lifecycle. By creating and adhering to the retention policy and schedule the university recognises that the creation and management of its information is essential for effective administration to meet strategic aims and objectives, to provide evidence of the activities of the university and to enable it to comply with legal and regulatory requirements.

## SCOPE

4. This policy applies to all staff, students and affiliates, including salaried and non-salaried staff, contractors, governors, students' union staff, honorary staff, collaborative partners and associates.
5. This policy applies to all information, whether digital or physical, processed by or on behalf of the University, for any purpose. This includes, including but is not limited to, information relating to:
    - teaching and learning
    - professional services and support functions
    - research and knowledge exchange, including externally funded projects
    - internal, and external, legal and regulatory reporting.

# POLICY

### Responsibilities

6. All staff and affiliates handle personal data, and some have specific roles in relation to data. Details of data roles are given in the Information Governance policy.
7. All members of staff are responsible for following this policy and for ensuring that they create accurate information that documents the actions and decisions for which they are responsible and maintain that information in accordance with the standards laid down in this document and for a period in line with the retention schedule. This includes storing information appropriately and securely, making sure electronic information is stored on an appropriate University system that is fully supported with an approved approach to backups.
8. All staff and affiliates are responsible for identifying redundant, obsolete and trivial information (ROT) and disposing of it in an appropriate, secure and, if necessary, an auditable manner in line with the University's Records Retention Schedule.

### Aims and benefits

9. The aim of this retention policy is to improve information management practice by creating a defined information lifecycle. This will result in the following outcomes:
    - Information will have authenticity, reliability, integrity and usability and therefore provide value to business processes and an accurate record of the university's business
    - Information will be stored within suitable storage systems, to facilitate retrieval and avoid unnecessary duplication
    - Access to information will be balanced with security appropriate to its level of confidentiality and importance
    - Information will be retained for the correct length of time and disposed of appropriately in line with the University's Records Retention Schedule.
10. These outcomes are in line with the concepts and principles set out in the 2016 international standard ISO 15489-1 on records management and the Lord Chancellor's Code of Practice under section 46 of the Freedom of Information Act 2000.
11. The benefits of this approach will be that the university can:
    - Exploit information effectively as a corporate resource in the delivery of teaching, research and corporate services
    - Work more efficiently including faster retrieval and access to the most up-to-date information
    - Retain the information it needs to by law including staff and student records, financial and environmental data, health and safety and contractual agreements

- Meet its obligations under the data protection legislation
- Provide evidence about policies and compliance, transactions, interaction with stakeholders and the rights and obligations of individuals and organisations
- Be better prepared in terms of business continuity and will be able to demonstrate previous compliance with correct procedures
- Free up storage space, both physical and electronic, effectively manage associated costs, and contribute to the university's sustainability agenda
- Retain and preserve information with continuing historical value or interest to the University and the wider world.

12. The aims and benefits above will contribute to wider information governance objectives and the mission of the university.

### Implementation and resources

13. Directorates and faculties will proactively implement and document procedures to ensure compliance with this policy and review them regularly. They will also be responsible for embedding good information housekeeping practices into processes that use information and keeping a record of these activities in the data audit logs. It is the responsibility of information asset owners e.g. data owners to ensure that the accuracy and relevance of information assets is maintained and that access to information is regulated by appropriate technical and organisational measures.

14. Non-university related personal information should not be stored on University premises or systems. It is strongly advised that any residual information that has no value or is no longer required for university purposes should routinely be removed from the relevant filing systems, drives, inboxes and other storage locations.

15. Information must not be destroyed where it is the subject of a complaint, legal dispute or a request under GDPR, FOI or EIR legislation. For example, under section 77 of the FOI Act it is a criminal offence to alter, conceal or destroy any information held by a public body to prevent its disclosure. It is therefore essential to follow procedures for the management of information. Documenting retention periods allows the University to demonstrate that information has been destroyed legitimately and not to prevent disclosure. Retention and disposal of records will be governed by the Kingston University Records Retention Schedule . The schedule provides a list of the records produced by the University and details of the length of time that they should be retained to meet operational and regulatory requirements.

16. Directorates and faculties will ensure that information is securely destroyed. For paper records this means that they should be disposed of using the confidential waste disposal service used by the University. Electronic records should be deleted, ensuring that all versions and copies are destroyed.

17. A small proportion of the university's information may be selected for permanent preservation in the university archives to be available for historical research and to give a lasting record of the university's business.

### Enquiries and Complaints

18. Any questions relating to data protection or how the University is processing personal data should be addressed to the University's Compliance and Information Governance team by email at dataprotection@kingston.ac.uk or by post to Compliance and Information Governance, Corporate Services, Holmwood House, Grove Crescent, Kingston upon Thames KT1 2EE.

19. Complaints should follow the Data protection complaint procedure under Information regulations on our Policies and regulations page.

## RELATED LEGISLATION, REGULATIONS AND POLICIES

20. Related legislation:

- Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000 (FOIA)
- Environmental Information Regulations 2004 (EIR)
- Limitation Act 1980

21. This policy should be read in conjunction with other relevant University policies and documents which can be viewed under Information regulations on our Policies and regulations page.

## BREACH OF POLICY

22. Anybody handling personal 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, and possible legal action.