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.

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 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.

5. This policy applies to all information held by the university in the course of carrying out its business, including research and the fulfilment of compliance with any regulatory requirements.

6. The information may be in any format or medium, including paper, structured datasets, unstructured documents, emails, texts and social media channels. It may also be stored, managed or hosted off-site by third party processors such as cloud-based software suppliers. Where that is the case, contractual agreements must ensure such arrangements comply with this policy and the relevant legislation.

POLICY

RESPONSIBILITIES

7. The Deans of Faculties and Pro Vice Chancellors and their Directorates or their nominated representatives are responsible to the Vice Chancellor and the University Secretary for the implementation of this policy within the university.

8. The University Secretary is responsible for ensuring the creation of the guidance for good information management practice and promoting compliance with this policy.

9. Local champions in each area of the University are responsible for promoting good practice and facilitating communication between their teams and the University Secretary's team in support of this policy, the retention schedule and other related issues including information, data protection and freedom of information.

10. 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, in particular making sure electronic information is stored on an appropriate University system that is fully supported with an approved approach to backups. It also includes 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 retention schedule. This policy applies to all information created, received or maintained by staff in the course of carrying out their duties, or by researchers engaged on internally or externally funded projects.

11. Other stakeholders that have access to the University's information must also be made aware of their responsibilities under this policy. This includes students, contractors, consultants, visitors and other affiliates. Where necessary this should include undertaking any mandatory training in relation to information management and data protection.

12. 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.

AIMS AND BENEFITS

13. 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 retention schedule.

14. 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.

15. 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 UK Data Protection Act including the General Data Protection Regulation (GDPR), the Freedom of Information (FOI) Act and the Environmental Information Regulations (EIR)
- 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.

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

RELATIONSHIP TO EXISTING POLICIES AND LEGISLATION

17. Directorates and Faculties should ensure that their information handling complies with any external guidelines, policies or legislation, including but not limited to the:

- GDPR, FOI and the EIR
- Requirements of professional bodies
- Requirements of national and international research funding bodies

- Requirements of any audits.

18. 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.

IMPLEMENTATION AND RESOURCES

19. 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.

20. 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.

21. Retention and disposal of records will be governed by the Kingston University 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.

22. Directorates and faculties will be prompted to review information at the appropriate time and, once records are approved for disposal, they will be securely destroyed. For paper records this means that they should be shredded with a cross-cut shredder or 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.

23. The relevant information asset owners in directorates and faculties will be given training on good practice and the retention schedule. Each area should ensure that the guidelines are followed. As required, these guidelines should be supplemented with additional local procedural documents as long as they reflect this policy and are reviewed regularly to consider any changes.

CONTACTS

24. To report a breach of this policy or a suspected or real personal data breach the University Data Protection Officer should also be notified immediately at dpo@kingston.ac.uk. The University Secretary's team should be contacted in relation to this policy and training, GDPR and FOI enquiries. The contact email address is: dataprotection@kingston.ac.uk.

RELATED LEGISLATION, REGULATIONS AND POLICIES

25. Related legislation:

- UK Data Protection Act 2018
- UK General Data Protection Regulation

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 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.