Records Management Policy

1. Policy statement

1.1 Context

This policy is a commitment from the University to take proper care of the records it holds and applies to all staff who work with these records.

Improvements in IT and our understanding of Information Risk Management has made Records Management an issue. Records Management is best approached as an integrated risk management issue.[1]

Records have a message, a medium and a context. Not all information is a record or needs saving but all information needs disposing of appropriately[2].

1.2 Regulatory context

This policy is part of implementing the Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (FOIA). This is referred to within this document as the section 46 Code of Practice. The standards in the Code apply to the University as a public authority. The Code takes a principles-based approach identifying value, integrity, and accountability as a framework for public authorities to manage information and maintain a record of their activities.

Appropriate, efficient and effective records management practice as an integral part of routine business processes should help the University to achieve its priority outcomes for delivering services and meet its statutory and evidential requirements, improving compliance and accountability with specific legal and regulatory requirements including health and safety legislation, finance legislation, the Freedom of Information Act 2000 (including the section 46 Code of Practice), the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (EU GDPR).

1.3 Prudent management principles

The UK GDPR sets out the fundamental data protection principles when processing personal information. Article 5(1) of UK GDPR requires that personal information:

(a) shall be used lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency' principle)
(b) shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation' principle)
(c) shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed ('data minimisation' principle)
(d) shall be accurate and, where necessary, kept up to date; ('accuracy' principle)
(e) that personal information is not kept in a form which permits identification of data subjects for longer than is necessary ('storage limitation' principle)

[1] Deloitte & Touche (2008)
[2] Penn

(f) is stored in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality' principle).

These principles must be applied to records constituting personal data (i.e., any information relating to an identified or identifiable living person)[3].

2. Policy objective

Records management is highly devolved across the University. This policy should be used by schools and departments as a foundation for assessing and improving their practices in order to maintain compliance with regulatory and legislative requirements in line with the University's wider objectives.

Information is an asset considered essential to the work of the organisation. Good records management is integral to the following aims and objectives:

Kent 2025 Strategy The University values excellence (page 4) and will be a leading civic university (page 5) and will be efficient and effective throughout our internal operations (Page 15). It will help facilitate performance improvement across all areas of education research, engagement and professional services. (Mid Term Review, page 14).

Planning and Data Engineering Aims: To support more effective and informed decision making throughout the University by the provision of timely and accurate management information.

Information Services Vision The IS vision is for a university with knowledge exchange and stimulation of creativity at its heart, where our community enjoys convenient and effective access to information and technology, and where we all work, learn and collaborate how and when it suits us, wherever we may be.

3. Scope

The policy applies to all records: student, academic, research and professional. It is irrespective of the technology used to create and store them or the type of information they contain. It includes, therefore, not only paper files but also business and information systems, e-mails and website content.

This policy aims to demonstrate that the creation, management and disposal of information assets has been carried out with proper authority, audit trail, agreed policy and risk assessment.

4. Definitions

Records are defined in the section 46 code of practice as follows: 'recorded information created, received and maintained as evidence and information by an organisation or person, in pursuit of legal obligations or in the transaction of business.'.

[3] Article 5(2) UK GDPR requires data controllers to be responsible for, and able to demonstrate compliance with these principles.

5. Records management

5.1 The role of records management

The role of records management is to facilitate the creation and management of authentic, reliable and usable records, capable of supporting business functions and activities for as long as they are required. It is an aid to corporate memory and should be applied to records generated in any format (e.g., paper, digital) from creation to disposal. The Code emphasises that public authorities must 'know what information they hold, why they hold it, how sensitive it is, and how it should be managed'.[4]

5.2 Requirements

Effective records management should ensure that records are complete, accurate, up to date, and accessible when required. The requirements of effective records management are to:

- identify which records should be created or received and retained
- capture and manage records through corporate record systems
- develop appropriate finding aids such as: meta data (information about information), classification schemes and indexes to facilitate the management and retrieval of information and records
- store records in appropriate, safe and secure environment(s)
- determine why and how long records should be kept and how they should be disposed of
- identify when information was created and who it was created by[5]
- retain records only for as long as they are needed to satisfy legal, regulatory, University or historical purposes
- ensure appropriate and routine disposal of records in line with University retention and disposal policies
- ensure routine disposal of ephemeral information (non-records).

5.3. Principles

Staff must ensure the following principles developed from the section 46 code of practice are followed. The records management guidance provided by the University links to these requirements.

Staff must ensure that records are	Good practice means:

[4] 1.2.3 Section 46 Code of Practice
[5] 2.4 Section 46 Code of Practice

valuable and trusted	• understanding, managing and using information in a way that enables it to understand its value, in order to make effective decisions[6] • being able to rely upon and trust the information held.
accessible & usable	• keeping records in systems that enable records to be stored and retrieved as necessary • knowing what records are held and where they are and ensuring that they remain usable for as long as they are required • taking action to conserve physical records if there are signs of damage and subjecting digital information subject to the appropriate above digital continuity[7] • ensuring appropriate tools consistently across the University to identify, locate & retrieve information required using an effective search capability and controls to protect sensitive information[8] • ensuring back-up systems to recover from system failures and major disasters[9].
kept only for as long as required	• keeping the accurate records needed for business, regulatory, legal and accountability purposes • defining how long to keep records, disposing of them when they are no longer needed and being able to explain why records are no longer held[10] • unless the University has assessed that it can be used for another purpose such as statistical, scientific, medical or historical research (subject to data protection legislation safeguards)[11] • destruction should be via a method appropriate to the security classification and proportionate to its sensitivity and security classification and certificated if by a contractor[12] • destruction/deletion should be permanent which means all known copies and versions, including back-up have been destroyed or deleted[13].
secure	• ensuring that records are stored securely and that access to them is controlled • by access and permission controls throughout the life of the information to prevent unauthorised or unlawful access[14]

[6] 2.13 Section 46 Code of Practice
[7] 2.3.6, Section 46 Code of Practice
[8] 2.3.9, Section 46 Code of Practice
[9] 2.2.5, Section 46 Code of Practice
[10] 2.3.1, Section 46 Code of Practice
[11] 2.3.2, Section 46 Code of Practice
[12] 2.7.6 – 2.7.7, Section 46 Code of Practice
[13] 2.7.8, Section 46 Code of Practice
[14] 2.4, Section 46 Code of Practice and

	• have appropriate technical and organisational measures to prevent accidental loss, destruction or damage[15].
shared correctly	• ensuring that records shared with other bodies or held on their behalf by other bodies are managed in accordance with the section 46 code of practice • ensuring a lead authority is agreed which will remain responsible for ensuring that information is managed in accordance with the section 46 Code of Practice[16] • the partner authorities recording in a data sharing agreement the obligation to record decisions, particularly in relation to the transfer or destruction of information, obligations under copyright, data protection legislation and FOIA, they record management controls and any special requirements for the security and handling of personal information and the ownership of any copyright[17].
accountability	• information management facilitates a clear and accurate account of activities in accordance with legal and other obligations[18].

5.4 Disposal [All formats]

Disposal does not necessarily mean destruction; it refers to activity when records are no longer required for university purposes and have reached their retention date. Disposal may include transfer for historical preservation.

Where destruction is appropriate records should be subject to confidential destruction and a disposal schedule maintained (containing the record name, destruction action and date).

5.6 Historical Preservation

Articles 5(1)(b) and 89 of UK GDPR allows 'processing in the public interest, scientific or historical research or statistical purposes.' Records identified as suitable for archiving should be transferred to the University Archive. Where practical, such information may be anonymised or pseudonymised.

6. Governance arrangements

6.1 The Senate

[15] ibid
[16] 2.8.1 Section 46 Code of Practice
[17] 2.8.2, Section 46 Code of Practice
[18] 2.1.3, Section 46 Code of Practice

- Lead responsibility for approving and supporting the implementation of this policy. It recognises that the University has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment.

6.2 Roles and Responsibilities for records management

The Senior Information Risk Owner (SIRO) currently Director of Governance and Assurance.

- Overseeing the management of the Information and Records Management function
- Overseeing the management of Information Risk and Governance.

Directors of Division or Assistant Directors (Operational responsible SIROs):

- Promote a proactive, positive culture of data protection compliance
- Revise and agree actions in respect of identified information risks
- Ensure senior management is briefed on information risk issues
- Ensure all information assets have an assigned Information Asset Owner
- Ensure that the division's approach to information risk is effective in terms of resource, commitment, and execution and that this is communicated to staff
- Own the risk assessment process for divisional information and cyber security risk, including review of annual information risks.

Directors of Division.

- Responsibility for the management of records generated by their activities, namely, to ensure that the records created, received, or processed within their purview, are managed in a way that complies with this policy. Keeping records of records disposed of including transfer for historical preservation.

The Data Protection Office shall:

- Draw up guidance for good records management practice and for supporting compliance with this policy
- act as Designated Manager for the purposes of the section 46 Code of Practice19
- develop and maintain University records management subsidiary policies
- identify the legal, regulatory, business authority under which records are kept
- document and authorise divergences from university retention schedules
- develop strategies with the University Archivist for the historical preservation
- identify and store copies of departmental Information Asset Registers.

Information Custodians shall:

- maintain a register of information assets in their area and ensure that they are included in the central Information Asset Register (held by the Data Protection Office).

Service Managers shall:

[19] 2.2.4 a designated manager of sufficient seniority to ensure that the University discharges its responsibilities under the Code, and that the authority is consistent in its approach to managing information, risk and access.

- ensure record keeping systems and records are managed to enable identification of records due for disposal
- keep records of information and records disposed of by their area20
- regularly identify and review records due for disposal to ensure they are no longer required
- ensure divergence from the University retention schedule is authorised
- ensure that staff are aware of policies to retain and dispose of records and only dispose of records in accordance with the University retention schedule
- ensure that records are disposed of appropriately by authorised staff21
- transfer records of potential historic interest to the archive for historical preservation with the agreement of the University Archivist
- engage with the DPO to make sure that information is managed in accordance with the section 46 Code of Practice before major organisational changes, before designing, developing, or procuring IT systems and applications and before entering cooperative arrangements with other public authorities or procuring services.[22]

All Staff (including Temporary Staff, Contractors and Consultants) shall:

- ensure that the records for which they are responsible form complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the University's records management guidelines and data protection policies.

7. Related documentation

This policy should be used in conjunction with the following policies and guidance:

Document	Description	Owner/Contact
Data Breach Policy	Details the procedure by which staff should report personal data breaches and the duty of staff to assist in the handling of breaches.	Data Protection Officer/Information Compliance Officer.
Data Protection Code of Practice	If you process personal data about individuals, you have a number of legal obligations to protect that information under the Data Protection Act2018. This document is intended as a brief guide to the Act and its implications for all members of University of Kent staff.	Data Protection Officer/Information Compliance Officer.
Data Protection Policy	If you process personal data about individuals, you have a number of legal obligations to protect that information under the Data Protection Act 2018. This document is intended as a brief guide to the Act and its implications for all members of staff.	Data Protection Officer/Information Compliance Officer.
Data Rights Policy	Written rules on access to the authority's information including personal information and other sensitive information.	Data Protection Officer/Information Compliance Officer.

[20] 2.6.2. Section 46 Code of Practice
[21] ibid
[22] 2.2.4 Section 46 Code of Practice

Document Retention and Archiving Policy	This policy sets out approved document retention periods in order that Kent may meet its obligations to students; comply with quality assurance requirements; reduce burdens on space and storage; and comply with the Data Protection Act by not retaining documentation longer than is justifiably necessary.	Quality Assurance and Validation Manager.
Records Retention Management Guide	Guidance and retention schedules for information held in higher and further education institutions.	Produced by the Joint Information Systems Committee (JISC).
Information Security Policy	Policy to ensure that the information managed by the University of Kent shall be appropriately secured.	Director of Information Services.
Archiving Policy Article 5 Transfer of Historical Records to Archive Control	Under development	University Archivist.
Copyright Policy and Guidelines	Policy, guidelines and links providing the fundamentals that you need to know about copyright and related rights at the University of Kent.	Copyright and Licensing Compliance Officer
Framework for Research Data Management (under development)	A sustainable framework for policy, services and systems that will support RDM at the University of Kent and enable effective data curation by researchers throughout the full data curation cycle.	Data Curator.
Freedom of Information	Written rules on access to the authority's information including personal information and other sensitive information	Data Protection Officer/Information Compliance Officer.

8. Monitoring and review

The University will review the content and effective implementation of this policy against the requirements of the section 46 Code biennially.

Managers should identify any risks related to records management (such as inappropriate hoarding, loss of information or non-compliance with the section 46 Code of Practice) as a result of organisational changes, sponsorship or procurement in their risk management registers and escalate high risks to senior management[23].

[23] 2.2.2 Section 46 Code of Practice requires a governance framework that takes account of information risks such as inappropriate hoarding and loss of information which provides for the involvement of senior management.

Document history

Version	Author	Description of Change	Date	Review date
1.0	Alan Martin	Policy created	Jan 2015	Jan 2017
2.0	David Bridge IDPO	Updated to reflect the requirements of good records management practice	Jan 2022	
2.1	Kate Kremers	Updated to reflect the requirements of the updated section 46 Code of Practice.	Mar 2022	Mar 2024

Version	Reviewed/Approved by	Approval date
1.0	Information Services Board	26 Jan 2015
1.0	Senate	11 Feb 2015
2.1	Information Services Committee	9 May 2022
2.1	EG with operational SIRO roles and divisional responsibility for records added to 6.2	6 June 2022
2.1	Audit committee – reviewed & noted.	14 June 2022
2.1	Academic Strategy, Planning & Performance Board discussed and recommended to Senate for approval	21 February 2023
2.1	Senate – reviewed and approved.	6 March 2023