Data Retention and Deletion Policy

Data Protection Officer
November 2023

UNIVERSITY OF
WINCHESTER

Document Title:	**Data Retention and Deletion Policy**
Document Author:	Stephen Dowell, Data Protection Officer
Responsible Person and Department:	Gavin Hunter, Chief Operating Officer
Approving Body:	University Leadership Team
Date of Approval:	November 2023
Date Effective From:	Immediately
Review Date:	December 2026
Indicate whether the document is for public access or internal access only **Indicate whether the document applies to collaborative provision?** *(Strikethrough text, as appropriate)*	**Public Access** **~~Internal Access Only~~** **~~Applies to Collaborative Provision~~**
Summary: This document sets out the Data Retention and Deletion Policy for the University of Winchester.	

Contents

Introduction

1. This policy is in place to ensure all staff (including temporary and contractors), visitors and students are aware of their responsibilities in relation to the University's approach to data retention and deletion and how it complies with the core principles of data protection.

2. Under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR), the University is classed as a data controller. To ensure that it complies with data protection legislation the University has appointed a Senior Information Risk Owner (SIRO) - this is assigned to the Chief Operating Officer- and a Data Protection Officer (DPO) and they have oversight of the detail of this policy.

3. The University recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the institution. Information held for longer than is necessary creates additional risk and cost, and breaches data protection principles.

4. Effective and adequate records, and data management is necessary to:

    a) Ensure that the University conducts itself in a structured, efficient and accountable manner.

    b) Reduce the risks associated with personal data and provide continuity in the event of a disaster or security incident.

    c) Ensure that the University realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems.

    d) Support University functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes.

    e) Meet legislative, statutory and regulatory requirements.

    f) Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner.

    g) Assist in document policy formation and managerial decision making.

    h) Protect personal information and data subject rights.

    i) Avoid inaccurate or misleading data and minimise risks to personal information.

    j) Erase data in accordance with the legislative and regulatory requirements.

Purpose and Scope

5. The purpose of this document is to provide University of Winchester's statement of intent on how it provides a structured and compliant data and records management system that facilitates the university's activities and provide evidence of transactions and functions.

6. Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

7. This policy applies to all staff within the University of Winchester[1]. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

Roles and Responsibilities

8. Deans, Directors, and Heads of Departments will have overall responsibility for the management of records and data generated by their departments' activities. They will be designated Information Asset Owners, but they may delegate this responsibility to a deputy or deputies. It will be their responsibility to ensure that the records created, received, and controlled within their department, and the systems and procedures they adopt, are managed in ways which meet the aims of this policy. **(See Appendix 1 for a list of information asset owners)**

9. It is the responsibility of the information asset owners to determine the retention periods for the information they collect. This determination should be made in line with any legal requirements associated with the purposes of processing. Advice and assistance can be sought from the data protection team.

10. Individual employees work with and contribute additional information to the University's data assets. Where this occurs, they are responsible for ensuring that the records are complete, accurate, maintained, and disposed of in accordance with University of Winchester's protocols.

Personal Information and Data Protection

11. The University needs to collect personal information about the people it employs, it works with, its students and the people it has a business relationship with, in order to carry out its business functions and activities, and to provide the products and services defined by our business type. This information can include (but is not limited to), name, address, email address, data of birth, IP address, identification number, bank details, confidential information, and sensitive information.

12. In addition, the University may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations. The University is committed to collecting, processing, storing, and destroying all information in accordance with UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

13. The University complies fully with the storage limitation principle as defined by Article 5 (1)(e)[2] of the UK GDPR:

> *"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')."*

[1] Meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the University in the UK or overseas.

[2] https://www.legislation.gov.uk/eur/2016/679/article/5

Objectives

14. It is the University's objective to implement the necessary records management procedures and systems which assess and manage the following processes:
    a) The creation and capture of records.
    b) Compliance with legal, regulatory, and contractual requirements.
    c) The storage and security of records.
    d) The protection of record integrity and authenticity.
    e) The use of records and the information contained therein.
    f) Access to and disposal of records.

15. Records contain information that are a unique and invaluable resource to the University and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals the information refers to. Records also serve to evidence University business functions and activities.

16. The University's objectives and principles in relation to Data Retention are to:
    a) Ensure that the University conducts itself in an orderly, efficient, and accountable manner.
    b) To only retain personal information for as long as is necessary.
    c) To develop and maintain an effective and adequate records management program to ensure effective archiving, review, and destruction of information.
    d) Support business functions and providing evidence of compliant retention, erasure, and destruction.
    e) Ensure the safe and secure disposal of confidential data and information assets.
    f) Comply with the relevant data protection regulations, legislation, and any contractual obligations.
    g) Ensure that records and documents are retained for their legal, contractual, and regulatory period stated in accordance with the rule or terms of each body.
    h) Ensure that no document is retained for longer than is legally or contractually allowed.

Guidelines & Procedures

17. The University manages records efficiently and systematically, in a manner consistent with data protection requirements, and this policy is widely disseminated to ensure a standardised approach to data management, retention and deletion.

18. Records will be created, maintained and retained to provide information about, and evidence of University transactions, customers, employment, and activities.

19. Retention schedules will govern the period that records will be retained. These schedules will be actioned and retained by relevant departments; the data protection team will also hold these schedules.

20. It is our intention to ensure that all records and the information contained therein is:

    a) Accurate.

    b) Accessible when necessary.

    c) Complete.

    d) Compliant.

    e) Reviewed.

    f) Secure.

Retention Period Protocols

21. All records retained during their specified periods are traceable and retrievable. All University student and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

22. For all data and records obtained, used and stored, the University will carry out periodic reviews of the data retained, checking the purpose of use, continued validity, accuracy and requirement to retain.

23. Where it is not possible to define a statutory or legal retention period, the University will make a business decision, in line with data protection principles, by which a period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices.

24. Processes will be in place to ensure that records pending audit, litigation or investigation are not destroyed or altered.

Designated Owners

25. All systems and records have designated owners throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, University area, and level of access to the data required.

26. Data and records are never reviewed, removed, accessed, or destroyed without the prior authorisation and knowledge of the designated owners. These owners will also be responsible for continually reviewing the retention schedule for items that they own, ensuring accuracy by updating the schedule accordingly if any retention periods or details have changed.

Document Classification

27. All departments will have a detailed Information Asset Register (IAR). These registers are used to document all assets containing personal data and the full life cycle of the data, including where the information comes from, who has access to it, who it is shared with, the duration of retention and deletion method. It is the responsibility of the IAR owners to review these registers on an annual basis. This ensures that they remain current, old assets are removed, and additional data assets are added in a timely manner.

Storage & Access of Records and Data

28. When stored and/or archived documents should be grouped together by category and in clear date order. Documents are always retained in a secure location, with access restricted to the authorised personnel.

29. Once the retention period has elapsed, the documents are either reviewed, archived, or confidentially destroyed depending on their purpose, classification, and action type.

Expiration of Retention Period

30. Once a record or data set has reached its designated retention period date, the designated owner should refer to their asset register for the action to be taken.

31. Not all data sets or records are expected to be deleted upon expiration; it may be sufficient to anonymise the data in accordance with data protection requirements or to archive records for a further period.

Destruction and Disposal of Records and Data

32. All information of a confidential or sensitive nature held by the University must be securely destroyed when it is no longer required. This ensures compliance with the data protection laws and the duty of confidentiality we owe to our employees, students, clients and customers.

Suspension of Record Disposal for Litigation or Claims

33. If the University is served with any legal request for records or information, or any employee becomes the subject of an audit or investigation, or we are notified of the commencement of any litigation against the University, the disposal of any scheduled records will be suspended until we are able to determine the requirement for any such records as part of a legal requirement.

Paper Records

34. Where the University retains personal information in a paper format, it has a duty to ensure that these are stored securely. Once the retention period is met, they should be disposed of in a secure, confidential, and compliant manner. The University utilises onsite shredding of all paper materials. Shredding machines and confidential waste sacks are made available to employees and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

Electronic & IT Records and Systems

35. The University uses numerous systems, and technology equipment in the running of its business. From time to time, such devices must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

36. University-provided devices (laptops, tablets, phones, etc.) must be returned to Knowledge and Digital Services (KDS) who will deal with the data removal. The device will then either be reissued or be handed to an outsourced company who will dispose of the device ethically and responsibly.

37. University data should not be routinely retained on personal devices. Where university data has needed to be stored on a personal device, it will be deleted as soon as it is no longer required to be held there.

Emails, Internal Correspondence, and General Memoranda

38. Unless otherwise stated in this policy or the retention periods schedule, correspondence and internal memoranda should be retained for the same period as the document to which they support (i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed). This supporting material must be stored alongside the principal documents(s) in the appropriate University storage location and retained in individual's files or email accounts.

39. Correspondence or memoranda that **do not** support any documents having already been assigned a retention period, should be deleted or shredded once the purpose and usefulness of the content ceases. Examples of correspondence and routine memoranda include (but are not limited to): -

    a) Internal emails.

    b) Meeting notes and agendas.

    c) General inquiries and replies.

    d) Letter, notes, or emails of inconsequential subject matter.

    Colleagues are reminded that emails are a transitory medium and that the University email system is not an additional storage space and should not be treated as such. Important material should be retained in a correctly managed file storage area that is not part of the email system.

40. When a portable storage device is found and handed to Reception/Security for safe keeping it will remain there for one calendar month. If after that period it has not been claimed, the storage device will be wiped and sent to the Multi-Media Centre for reuse.

Erasure

41. In specific circumstances, a data subject has the right to request that their personal data is erased. However, the University recognises that the 'right to be forgotten' is not absolute. The right to have personal data erased and to prevent processing

only applies:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

b) When the individual withdraws consent (when the personal data is collected under this lawful basis.)

c) When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

d) The personal data was unlawfully processed.

e) The personal data must be erased to comply with a legal obligation.

f) The personal data is processed in relation to the offer of information society services to a child.

42. Where the University receives a request to erase data the first step will be to determine which data sets the right of erasure applies to, if any. If the right does apply, the erasure will be carried out under instruction of the Data Protection Officer in conjunction with the relevant departments to ensure that all data relating to that individual has been erased. Erasure should take place within 30 days of the request being received.

43. Whilst standard procedures already remove data that is no longer necessary, a dedicated process will be followed for erasure requests to ensure that all rights are complied with, and that no data has been retained for longer than is needed[3].

44. If for any reason, the University is unable to act in response to a request for erasure, a written explanation will be provided to the individual and inform them of their right to complain to the Supervisory Authority and to seek a judicial remedy.

Special Category Data

45. In accordance with data protection law, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc. The University's methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data.

Compliance and Monitoring

46. The University is committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

[3] Where the University of Winchester has made any of the personal data public and erasure is granted, it will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data.

Appendix: Information Assets

Department	**Sub-Departments**	**Designated Information Asset Owner**
Marketing, Communication & Engagement		**Director of Marketing, Communication & Engagement**
	External Engagement & Partnership (Alumni)	Head of External Engagement & Partnerships
	Marketing	Director of Communication & External Relations
	Admissions	Head of Admissions & Customer Insight
	International Recruitment	Head of International Recruitment
	Student Recruitment	Head of Admissions & Customer Insight
Estates & Facilities Services		**Director of Estates & Facilities Services**
	Campus Management	Head of Facilities & Business /Campus Manager
	Catering	Catering Operations Manager
	Conferences	Conferences & Reception Services Manager
	EFS Management	EFS Administration Manager
	Energy & Environment	Head of Environment & Building Services
	Front of House (Reception)	Reception Services Supervisor
	Health & Safety & Business Continuity	Health, Safety & Business Continuity Manager
	Housing	Head of Housing & Security
	Maintenance	Head of Environment & Building Services
	Project & Estate Management	Head of Projects & Estate Management
	Security	Head of Housing & Security
	Sport Facilities	Sports Facilities Development Manager
	Timetabling	Timetable & Room Bookings Manager
Faculty of Business & Digital Technologies		**Director of Faculty Operations**
Faculty of Education & Arts		**Director of Faculty Operations**
Faculty of Health & Wellbeing		**Director of Faculty Operations**
	Winchester Health Clinic	Physiotherapy Clinic Manager
Faculty of Humanities & Social Services		**Director of Faculty Operations**
Faculty of Law, Crime & Justice		**Director of Faculty Operations**
Finance & Planning		**Director of Finance & Planning**
	Finance	Deputy Director of Finance (Financial Services)

	Planning	Head of Planning
Human Resources		**Director of Human Resources & Payroll**
	HR & Payroll	Director of Human Resources & Payroll
	Staff Development	Director of Human Resources & Payroll
	Equalities	Director of Equalities
Knowledge & Digital Services		Director of Knowledge & Digital Services
	ITS	Director of Knowledge & Digital Services
	Library	Head of Knowledge Services
Research & Innovation		Director of Research and Innovation
	Business Development	Director of Research and Innovation
	Centre for Real World Living	Director of Research and Innovation
	PGR	Doctoral School Manager
	WCRRP	Director of CRRP
Registry & Academic Quality		**Academic Registrar**
	Academic Quality	Head of Quality
	Registry	Assistant Academic Registrar
	Complaints	Head of Complaints & Casework
	Learning & Teaching Development Unit	Head of Technology Enhanced Learning & Digital Literacies
Senior Management Group		**Senior Information Risk Owner/Chief Operating Officer**
	Chaplaincy	Chaplain
	Governors	Clerk to the Board
	Data Privacy	Data Protection Officer
	Continuous Improvement Unit (CIU)	Head of CIU
	Senior Management Support (SMT)	Head of the Vice-Chancellor’s Office
Student Support & Success		**Director of Student Support and Success**
	Student Engagement & Employability (Careers)	Head of Graduate Success
	Student Support (Student Services)	Director of Student Support and Success
	Widening Participation	Head of Participation & Success