

DATA RETENTION POLICY

Introduction

1. The aim of this Policy is to ensure that records are managed consistently across the University and that they are retained for as long as necessary to meet operational and business needs, and to demonstrate compliance with legal, regulatory and audit requirements. It applies to all records in whatever format they are held (i.e. paper or electronic). The retention schedules to which this Policy refers also take into account relevant requirements of the University's regulations and policies. This Policy should be read in conjunction with the Data Deletion Process.
2. This Policy covers both digital and paper/physical data, all should be processed securely and in accordance with the University Acceptable Usage Policy.
3. Given the cost and the environmental impact of storing and backing up digital data, particularly media-rich content, the University does not wish to retain data longer than necessary if it is no longer being accessed.
4. The University is bound by various legal obligations relating to data retention, meaning certain classes of data must be stored for specified lengths of time before deletion. Such obligations include but are not limited to:
 - 4.1 UK General Data Protection Regulation (GDPR) for personal data
 - 4.2 HMRC guidance for financial records
 - 4.3 Office for Students and Middle States Commission on Higher Education requirements for academic, financial and other records
 - 4.4 Family Educational Rights and Privacy Act (FERPA)
5. Unless otherwise stated, it is the responsibility of departments to retain the items listed in the schedules and within the departments themselves specific individuals should be assigned responsibility for each category, known as Data Owners.

Scope

6. This policy applies to all University employees, including part-time, contracted and associate staff, and to all registered students.

7. This policy applies to all data which is the property of the University, and/or forms part of a student's submitted assessment or coursework, and/or which is stored on University storage platforms. Such platforms include, but are not limited to:
 - 7.1 Microsoft Teams, OneDrive, SharePoint
 - 7.2 University Email accounts
 - 7.3 BlackBoard
 - 7.4 Filing cabinets
8. This policy does NOT apply to data stored in locations that are not covered by the University's backup solution and/or contractual arrangements between the University and external third parties. Where data is restored through backup it will require a further review by the Data Owner to ensure it does not exceed its data retention periods as defined in this policy. The University does not guarantee to backup or retain data stored in unsanctioned locations. Such locations include, but are not limited to:
 - 8.1 Storage on individual computers or laptops, as opposed to file servers.
 - 8.2 Third party cloud-hosted storage solutions (other than Microsoft OneDrive, Teams and SharePoint,) including Adobe CreativeCloud, DropBox, etc.
 - 8.3 Any form of removable storage, including portable hard disks, USB keys and CD/DVD disks, even if owned by the University.

Data Retention Periods

- The tables below show the duration for which data must be retained by the University.

Human Resources – DATA OWNER Deputy Vice-Chancellor, Finance and Operations

Data Process	Data Type	Retention	Justification
Income tax and NI records	Personal data	3 years from the end of financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Payroll wage/salary records (also overtime, bonuses, expenses)	Personal data	6 years from the end of the tax year to which they relate	Taxes Management Act 1970
Leave, including Leave forms, holidays, sickness, Deductions Working Sheets, Statutory Maternity, Paternity and Sick Pay records National Minimum Wage records	Personal data	3 years post leaving employment	Administration) Regs 2002, reg. 9 + Additional Statutory Paternity Pay (Birth, Adoption and Adoption from Overseas) (Administration) Regs 2010 (SI 2010/154), reg.9 NB: Statutory Sick Pay (Maintenance of Records) (Revocation) Regs 2014, in force from 6th April 2014, revoke Reg 13 of the 1982 Regs which provides for records concerning payments of SSP to be retained by employers. Note that under the Deduction from Wages (Limitation) Regs 2014 there is a 2-year time limit for backdated claims

Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	Personal data	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	Personal data	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Working time records	Personal data	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)
Personnel records	Personal and Sensitive data (special category)	6 years after the employee has left	To defend against tribunals or county or high court claim
Employee training records	Personal and Sensitive data (special category)	6 years after the employee has left	Health and safety, fire precaution regulations
Recruitment records (including DBS checks)	Personal data	6 months after the candidate has not been successful	To defend against tribunals or county or high court claim
Emails and personal data volumes (across all University systems)	Personal and Sensitive data (special category)	6 months after the employee has left	To answer queries that are contained in these data sources
Teaching records of Faculty			

Event registrants and participants – DATA OWNER Director of Marketing Recruitment and Communications

Data Process	Data Type	Retention	Justification
Ad-hoc events	Personal and Sensitive data (special category including accessibility, dietary and allergy details)	5 years post last interaction with individual	To maintain a record of them and their interactions with the University to answer any queries or concerns
Annual events	Personal and Sensitive data (special category including accessibility, dietary and allergy details)	18 months after event for personal data, 2 months after event for sensitive data (special category).	To maintain a record of event attendees and reinvite those that attended
Event Permits and licenses	Personal data	6 months after the permit expires	To retain a record of permits and licenses held
Event speakers	Personal data, may include bios	5 years post last interaction with individual	To maintain a record of them and their interactions with the University to answer any queries or concerns

Student records – DATA OWNER Academic Registrar

Data Process	Data Type	Retention	Justification
Student File (including admissions information)	Personal and Sensitive data (special category including health conditions and conduct concerns)	6 years	To ensure information is available in case of enquiries, audits, requests for references, disputes or litigation; Limitation Act 1980; Data Protection Act 2018; JISC recommendation; common practice within higher education.

Admissions records for unsuccessful candidates	Personal data	6 months post conclusion of the admissions process	To provide the candidate with responses post any queries and to defend any decisions made during this process.
Student (including Exchange) Transcript	Personal data	Permanent	To provide a service to the former student throughout his/her lifetime and to preserve the historical record of the awards of the University.
Student Diploma Supplement	Personal data	Permanent	To provide a service to the former student throughout his/her lifetime and to preserve the historical record of the awards of the University.
Virtual Learning Environment and other University System student data (Postgraduate and Undergraduate)	Personal data	5 years post-graduation	Requirement of the Office for Students
Non-credit student data	Personal data	2 years post course completion	To provide answers to student queries and evidence
Enquirers	Personal data	2 years post completed enquiry	To be able to answer the enquiry and promote the enquirer to an applicant
Alumni contact data	Personal data	In perpetuity	To manage the relationship with the alumni member
Partner University Exchange and Study Abroad Student Data	Personal and Sensitive data (special category including health conditions and conduct concerns)	6 years	To ensure information is available in case of enquiries, audits, requests for references, disputes or litigation; Limitation Act 1980; Data Protection Act 2018; JISC recommendation; common practice within higher education.

Estates and Facilities – DATA OWNER Head of Estates and Facilities

Data Process	Data Type	Retention	Justification
Environmental planning, incidents, audits, assessments, registrations and licenses, reports, Geo/environmental site investigation reports	Personal data	Permanent	Based upon alignment to the Construction and Estates retention rules; this exceeds the 30-year time limit for the recovery of, and security for, the cost of remediation by the enforcing authority within The Environment Act 1995 and Environmental Protection Act 1990.
Maintenance, Repairs, Plant and Equipment Tests (including PAT (Portable Appliance Testing), gas, electrical, air, lift, roof fans, water quality, alarms, sprinklers, extinguishers, fireman's switches, dry risers, emergency lighting, lightning protection)	Personal data	Permanent	Supports 15 years long stop within the Limitation Act 1980 (c. 58, s. 14B) for latent damage for actions relating to property
University campus attendee accident record	Personal and Sensitive data (special category including health conditions)	3 years post the incident (3 years post turning 18 of any young people)	In alignment with HSE requirements and RIDDOR
University campus visitors, including staff	Personal data	2 months post last entry	To retain access logs for health and safety and crime prevention
CCTV footage	Personal data	29 days	To provide evidence of crime or to assist safety investigations

Access control records (students, staff and visitors)	Personal data	41 days	To provide evidence of crime or to assist safety investigations
--	---------------	---------	---

IT – DATA OWNER Head of IT

Data Process	Data Type	Retention	Justification
Key system access and security logs	Personal data	12 months	To provide evidence in forensic investigations

Finance – DATA OWNER Head of Finance

Data Process	Data Type	Retention	Justification
Annual accounts	Records documenting the preparation and submission of Annual statutory accounts.	7 years	Limitation Act 1980, s.5; Taxes Management Act 1970, s.34
Records of capital assets and decisions to dispose of them	Inventory; Asset register; Disposal forms	7 years	Limitation Act 1980, s.5; Taxes Management Act 1970, s.34
Management accounting	Monitoring income and expenditure against annual operating budgets; Action to deal with variances; Analyses of internal deployment of financial resources.	7 years	JISC guidelines
Budgeting	Records documenting the preparation of annual operating budgets.	7 years	JISC guidelines

Tax returns and VAT	Records documenting the preparation and filing of the institution's tax returns; Records documenting the institution's accounting for VAT.	7 years	Taxes Management Act 1970, s.34; Value Added Tax Act 1994, s.58, sch11, para. 6(3); SI 1995/2518 s.31; HMRC 700/21 para. 2.4
Records documenting the administration of bank accounts	Standing orders; Direct debit mandates; Paying-in and withdrawal slips.	7 years	Taxes Management Act 1970, s.34; Limitation Act 1980, s.5
Purchases and incoming payments (including student fees and records of Financial Aid)	Invoices; Credit notes; Delivery notes; Income and expenditure batches; Receipts; BACS reports; Till rolls; Petty cash records; Payment of accommodation fees.	7 years	Taxes Management Act 1970, s.34; Limitation Act 1980, s.5; Value Added Tax Act 1994, s.77(1); HMRC 700/21 para. 2.4
Expenses	Records documenting the payment and/or reimbursement of expenses.	7 years	Taxes Management Act 1970, s.34; Limitation Act 1980, s.5.

Research funding	Allocations from statutory funding councils; Research project applications, award letters, invoices.	7 years	Limitation Act 1980, s.5.
Internal accounting	Records documenting administration and processing of Inter Departmental Transfers (IDT's) and (IDJ's).	1 year	JISC Guidelines
Investment management	Fund managers' reports; Records of purchase and sale of investments.	7 years	Limitation Act 1980, s.5; Taxes Management Act 1970, s.34.
WPM Richmond Store	Financial transactions and user accounts	7 Years	HMRC 700/21 para. 2.4

Library DATA OWNER Head of Library Service

Data Process	Data Type	Retention	Justification
Book requests and circulation history	Personal data	18 months post departure	To allow for students and employees on leave of absence or studying abroad.
Fines	Personal data	18 months post departure	Full student record maintained during enrolment.
Inter library loans	Personal data	3 years	To allow for inter-year and comparative and trend analysis
Purchase requests	Personal data	3 years	To allow for inter-year and comparative and trend analysis
Scan requests	Personal data	3 years (retained for faculty/class distribution requests only)	To ensure compliance and allow inter-year and comparative and trend analysis

Responsibilities

9. It is the responsibility of individual employees and students to ensure their data (if covered by this policy) is stored in an approved location, so its retention can be guaranteed, and therefore avoid inadvertently creating a breach of this policy. The Data Owner is the custodian of the data. They're responsible for the data created and maintained in their work area, including highlighting when data should be reviewed or retired. One individual is elected from each department.
10. The IT Department is responsible for ensuring the safe retention of data for as long as is required by this policy, and for arranging its secure destruction at the end of its retention period on the say so of the Data Owner.

VERSION MANAGEMENT

Responsible Department: IT			
Approving Body: University Board (on recommendation of Operations Committee)			
Version no.	Key Changes	Date of Approval	Date of Effect
1.0	Initial Version	24 July 2025	September 2025
1.1	No changes to the plan; reviewed and approved by University Board for AY 2026–27.	05 May 2026	September 2026
		Restricted Access? <i>Tick as appropriate:</i> Yes ☐ No ☒	