Records Management and Data Retention Policy

Policy no:	DIG 2.4
Version no. & date:	Version 3.2 – 23 October 2026
Author:	Academic Registrar (Designated DPO)
Policy Owner	Chief Academic Officer
Last review date:	23 October 2026
Next review due:	October 2028
Responsible Committee:	College Management Team (CMT)
Approved by & date:	College Management Team (CMT) – 23 October 2026
External reference points:	UK GDPR (2018) Data Protection Act 2018 Data (Use and Access) Act 2025 The Limitation Act 1980 Companies Act 2006
Linked policies:	DIG 2.1 Data Protection and Confidentiality Policy; DIG 2.7 Subject Access Request and Individual Data Rights Policy
Audience:	All Staff

1. Purpose

This policy establishes the framework for the systematic management of records and retention of data at UK College of Business and Computing (UKCBC or the College). It ensures the College complies with legal, regulatory and operational requirements while maintaining efficient, secure and accountable information management practices throughout the lifecycle of institutional records.

2. Scope

This policy applies to all staff at UKCBC and covers all records created, received, maintained or disposed of by the College in any format, including physical and digital records. It encompasses organisational, academic, student, financial, staff, partner and agent records.

3. Definitions

Anonymisation: The irreversible removal of personal identifiers from data so that individuals can no longer be identified.

Archiving: The permanent preservation of records that have enduring historical, legal or operational value.

Data Retention: The College's approach to determining how long records are kept, based on legal, regulatory and operational requirements.

Data Subject Access Request (SAR): A request from an individual to access their personal data held by the College under UK GDPR.

Disposal: The secure and irreversible destruction of records that have reached the end of their retention period.

Personal Data: Information relating to an identified or identifiable living individual, as defined under UK GDPR.

Pseudonymisation: The processing of personal data in such a way that it can no longer be attributed to a specific individual without the use of additional information, which is kept separately. Pseudonymised data remains personal data under UK GDPR.

Record: Information created, received or maintained by UKCBC as evidence of business activities, regardless of format.

Records Management: The systematic management of records throughout their lifecycle, from creation to disposal or archiving.

Retention Period: The specific length of time a record must be retained before it may be disposed of or archived.

4. Roles and Responsibilities

4.1 All Staff

All staff, including managers and those in leadership positions, have a responsibility for the proper use, retention, privacy and security of information. Staff must ensure that records are created, maintained, stored and disposed of in accordance with this policy and relevant legal requirements.

4.2 Data Protection Officer (DPO)

The DPO is responsible for managing the Data Subject Access Requests (SAR) process with the support of departmental managers. The DPO leads on monitoring developments in legislation and good practice relevant to data protection and records management.

4.3 People and Culture

People and Culture is responsible for training, induction materials and information provided to staff via the Human Resources (HR) system to ensure staff are aware of their responsibilities. HR maintains the retention and privacy arrangements for staff and supplier records.

4.4 MIS Manager

The Management Information Systems (MIS) Manager is responsible for the student lifecycle, retention and privacy arrangements within business applications and for coordinating the quarterly action plans. The MIS Manager provides resources for the development of automated processes and reports to support compliance with this policy.

4.5 Head of IT

The Head of IT is responsible for providing relevant resources, managing email and directory applications, and maintaining network infrastructure. The Head of IT is responsible for ensuring that this policy is applied to digital data store infrastructure, back-up, test and other environments and holds specific responsibility for the security of the College's digital systems.

4.6 Operations Committee

The Operations Committee holds institutional responsibility for information governance and management at UKCBC. The Committee provides governance oversight of this policy, including approval of the policy and its associated Records Retention Schedule, and receives assurance reports on retention schedule compliance through the committee reporting cycle.

4.7 Department Heads

Department Heads are responsible for implementing this policy within their areas, ensuring staff compliance, and making decisions on the archiving or destruction of records at the end of specified retention periods.

Role	Responsibility Area
All Staff	Record creation, maintenance, storage and disposal compliance
DPO	SAR management; legislative and good practice oversight
People and Culture	Staff and supplier retention; training and induction
MIS Manager	Student lifecycle systems; automated processes and reporting
Head of IT	Digital infrastructure security; email and directory systems
Department Heads	Local implementation; end-of-retention decisions
Operations Committee	Policy approval; governance oversight; assurance on retention schedule compliance

5. Policy Statement

5.1 General Principles

UKCBC is committed to managing records in a systematic, secure and compliant manner. The College retains records only for as long as necessary to fulfil legal, regulatory, operational and business purposes. Records that have reached the end of their retention period must be disposed of securely or archived where they have enduring value.

5.2 Legal and Regulatory Compliance

The College complies with all relevant legislation governing records management and data retention, including UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, the Limitation Act 1980, and the Companies Act 2006. Retention periods specified in this policy are informed by legislative requirements and sector best practice.

5.3 Data Protection Principles

Personal data must be retained in accordance with UK GDPR principles, including storage limitation. The College retains personal data only for as long as necessary for the purposes for which it was collected. Where personal data is no longer required, it must be securely deleted or anonymised.

5.4 Security and Confidentiality

All records must be stored securely throughout their lifecycle. Access to records containing personal or sensitive information must be restricted to authorised personnel only. Records must be disposed of securely to prevent unauthorised access or disclosure.

5.5 Archiving and Permanent Retention

Records that have enduring historical, legal or operational value must be preserved permanently. Department Heads are responsible for identifying records suitable for archiving at the end of their active retention period.

6. Records Retention Schedule

The College maintains a detailed Records Retention Schedule that specifies retention periods for different categories of records. The schedule is informed by legislative requirements, regulatory expectations and sector best practice. Retention periods may vary where there are particular legislative or statutory requirements.

The Records Retention Schedule is structured by the following categories:

- Organisational Records
- Marketing and Recruitment Records
- Agent Records
- Student Records (including Applicants and Alumni)
- Financial Records
- Staff Records
- Partner Records
- Other Individual Records

Full details of retention periods for each category are maintained in the Records Retention Schedule, held on SharePoint and accessible to all managers. The Records Retention Schedule is the single authoritative source of retention information for the College. Retention periods contained within it are aligned with those referenced in DIG 2.1 Data Protection and Information Governance Policy (v6.0). Where any discrepancy exists between this schedule and DIG 2.1, the Policy Owner must resolve it and ensure both documents reflect a consistent position before the next scheduled review. Any amendments to the schedule must be authorised by the Chief Academic Officer and recorded in the schedule version history. The Chief Academic Officer must ensure, through the DPO governance structure, that the Records Retention Schedule and all supporting disposal documentation are complete, current and operationally maintained. Findings and assurance outcomes must be reported to the Operations Committee through the committee reporting cycle to confirm the effectiveness of retention controls and supporting documentation. The Operations Committee reviews compliance with the retention schedule as part of its oversight of the Data and Information Governance policy suite.

7. Procedures

7.1 Record Creation and Maintenance

Staff must create accurate, complete and reliable records of business activities. Records must be stored in authorised data stores and software systems as set out in the College's 'Data Stores and Contracts' document, maintained by the Head of IT. Staff must not create or maintain records in unauthorised locations.

7.2 Retention Period Review

At the end of the specified retention period, Department Heads must review records and determine whether they should be destroyed or retained for archival value. The date and action taken (destruction or archiving) must be recorded.

7.3 Secure Disposal

Records approved for disposal must be destroyed securely and irreversibly. Physical records must be shredded or otherwise destroyed to prevent reconstruction. Digital records must be permanently deleted using secure deletion methods.

Disposal must be evidenced as follows:

- Physical records destroyed by an approved contractor must be accompanied by a destruction certificate, retained by the relevant Department Head.
- Physical records destroyed on-site must be recorded in a witnessed destruction log, noting the record category, date and authorising officer.
- Digital records deleted from college systems must be recorded in a deletion log maintained by the Head of IT, noting the system, record category, date and authorising officer.
- Where records held by third-party processors are deleted, written confirmation of deletion must be obtained from the processor and retained by the DPO.

Disposal records must be retained for a minimum of six years.

7.4 Anonymisation

Where records have ongoing operational or research value but contain personal data that is no longer required, the College may anonymise the records rather than destroy them. Anonymisation must be

irreversible so that individuals can no longer be identified, directly or indirectly, by any means reasonably likely to be used.

Staff must not treat pseudonymised data as anonymised. Pseudonymised data remains personal data under UK GDPR and must continue to be managed in accordance with this policy and DIG 2.1.

Before anonymised data is treated as falling outside the scope of UK GDPR, the DPO must confirm in writing that the anonymisation is effective and irreversible. This confirmation must be recorded and retained as evidence of compliance.

7.5 Exceptions to Retention Periods

Records subject to ongoing legal proceedings, investigations, audits or Data Subject Access Requests must be retained beyond their normal retention period until the matter is resolved.

Where a legal hold is required, the following process must be followed:

- Initiation: The DPO initiates the legal hold as soon as they become aware of proceedings, an investigation, audit or SAR that affects specific records.
- Recording: The DPO records the hold in writing, noting the record categories affected, the reason for the hold, the date of initiation and the anticipated resolution date.
- Communication: The DPO notifies the relevant Department Heads and the Head of IT in writing, ensuring that affected records are identified and preserved across all relevant data stores.
- Lifting: Once the matter is resolved, the DPO confirms the hold is lifted in writing and notifies all relevant parties. Records are then returned to their normal retention schedule and disposed of in accordance with Section 7.3 where their retention period has expired.

No records subject to a legal hold may be disposed of without the DPO's written authorisation.

7.6 Routine Destruction of Records

Certain records have no significant operational, informational or evidential value and may be destroyed as soon as they have served their primary purpose. These include:

- Meeting announcements, notifications of acceptance or apologies
- Requests for standard information such as maps, travel directions and brochures
- Requests for and confirmations of reservations for internal services (e.g. meeting rooms)
- Transmission documents, including email messages, instant messages and digital communications that do not contain decisions, commitments, instructions or substantive business information
- Superseded address lists and distribution lists
- Duplicate documents including copies marked "CC" and "FYI"
- Unaltered drafts where a final version exists
- Snapshot printouts or extracts from databases
- Working papers where results have been incorporated into an official document
- Obsolete or superseded stocks of in-house publications
- Automated system notifications and alerts that require no action or record
- Calendar invitations and scheduling confirmations

When a communication becomes an official record

A communication becomes an official record, regardless of the channel or format in which it was sent, when it contains a decision, commitment, instruction or substantive information relevant to college business. Staff communicate with students primarily via email, telephone and the eVision Student 360

portal. Substantive communications through all three channels are logged within eVision, which is an authorised data store. Official records must be stored in an authorised data store in accordance with Section 7.1 and are subject to the retention periods set out in the Records Retention Schedule.

8. Monitoring and Review

The Chief Academic Officer monitors compliance with this policy and coordinates reviews of the Records Retention Schedule through the DPO governance structure. The policy and associated Records Retention Schedule are reviewed at least every two years, or earlier if required by legislative, regulatory or operational changes. The MIS Manager coordinates automated processes and reports to support monitoring and compliance. Assurance on the completeness, currency and operational maintenance of the Records Retention Schedule and supporting disposal documentation is reported to the Operations Committee through the committee reporting cycle.

9. Linked Policies

This policy should be read in conjunction with:

- DIG 2.1 Data Protection and Information Governance Policy v6.0
- Records Retention Schedule (supplementary schedule to this policy, held on SharePoint)
- DIG 2.7 Subject Access Request and Individual Data Rights Policy
- DIG 2.6 Information Security and Acceptable Use Policy

10. External Reference Points

This policy has been developed with reference to:

- UK General Data Protection Regulation (UK GDPR) 2018
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- The Limitation Act 1980
- Companies Act 2006
- Information Commissioner's Office (ICO) Guide to UK GDPR: Storage Limitation (Article 5(1)(e)), available at ico.org.uk

Version History

Version	Date	Author	Summary of changes	Approved by
1.0	Dec 2020	Ben Stedman	Initial Retention Policy created	
2.0	June 2025	Ben Stedman		
3.0	February 2026	Pauline Williams	Comprehensive revision to align with GA 3.1 Policy Preparation and Structure Guidance, enhanced committee structure, strengthened procedures Key changes include strengthened compliance through updated legislation, correct committee assignment and a compliant review cycle; improved clarity via active voice, plain English, expanded definitions and consistent terminology; enhanced information accuracy through refined scope and purpose, corrected legal references, restructured retention content and removal of outdated or operational detail.	
3.1	June 2026	Pauline Williams	Governance review: updated approving body to Operations Committee throughout (sections 4.6, 6, 8, frontispiece) in line with Review and Approval Framework; updated DIG 2.1 cross-references to v6.0 consolidated title; added governance assurance language to sections 6 and 8 confirming DPO-led review and Operations Committee reporting arrangements for the Records Retention Schedule; clarified Records Retention Schedule as single authoritative source; updated linked policies (section 9) to remove superseded standalone schedule references.	
3.2	23 October 2026	Chief Academic Officer	Role titles updated following organisational restructure; front sheet, footer and cross references updated for approval; approved by College Management Team (CMT) on 23 October 2026 Abbreviations spelt out at first use in line with GA 3.1 (25 October 2026). Version	College Management Team (CMT)

Version	Date	Author	Summary of changes	Approved by
			History table aligned with the suite (26 October 2026).	