BURY COLLEGE

Bury College Policy and Procedures

Data Retention Policy

Document Retention and Disposal Policy

General Statement

Bury College is committed to the robust and efficient management of its records which are necessary to support its core functions. In particular the College commits:

- to comply with its legal and regulatory obligations, particularly in relation to the UK General Data Protection Regulation (UK GDPR) and Data Protection Act (2018), The Privacy and Electronic Communications Regulations (PECR) and the Freedom of Information Act 2000 (FOI) (As Amended)
- Where relevant, we will aim to comply with the standards of the Age-Appropriate design code when processing, retaining, and disposing of information.
- to ensure that records are held with the appropriate degree of security.
- to ensure records are held and archived for the minimum required period and disposed of appropriately.
- to make clear the specific responsibilities of each member of staff in relation to the management of and access to records

This policy applies to all records created, received or maintained by College staff in the course of carrying out their functions as College employees. This policy applies to both manual/physical and electronic records. Procedures for dealing with requests for personal and corporate records are provided in the College's Data Protection and Freedom of Information Policies.

Definitions

Records are defined as any documents used by the College, which are retained (for timescales set out below) to provide evidence of any aspect of its business. These records may be created, received or maintained Physically or electronically.

Records Management is concerned with providing clear guidance on the control, creation, maintenance, use, storage and disposal of records. This encompasses the processes involved in the creation, dissemination, gathering and maintaining information about the College's activities that result in the formation of records.

Policy Statement

The College will maintain its records and record keeping systems in accordance with current legislation.

The College will ensure that nominated Heads of Areas are assigned the role of Records Coordinator to ensure that systems and procedures are compliant and managed effectively so records can be retrieved easily in a timely fashion. This relates to manual records only. The management, retention and destruction of electronic records will be the responsibility of the Head of MIS, Head of IT Services and Director of HR.

Individual College departments will ensure that they clearly identify the records for which they are responsible, that they are accurate, and that they are maintained and disposed of in accordance with the records management guidelines maintained by the Records Managers.

All records within a department should have an identified owner responsible for their management whilst in regular use.

Each department will produce clear procedures on the storage, security and archiving of records for which it is responsible.

All members of staff should receive a briefing on records management procedures as part of their induction programme.

The College will provide appropriate facilities for storing and retrieving archived records, and for their destruction at the appropriate date.

KPI Measures

Production and regular review of College Record Management Guidelines.

Production and regular review of Departmental procedures; (Finance, Principalship, HRM, Business Development, Physical Resources, MIS & Curriculum).

Proportion of archived records destroyed by their due date.

The proportion of requests for information under the provisions of the Data Protection and Freedom of Information Policies, dealt with in the specified timescales.

Procedures for Implementing the Policy

College Records Management Guidelines.

1. Document classification

Each department should provide guidance on classifying documents it holds, and how to implement these procedures. Support for the process is available from the Records Manager.

Record will be categorised into one of two categories of classification: **Confidential** and **Non/Permanent**.

- Confidential documents are those which either contain information linking them to specific individuals (usually because they contain names or addresses), or information which is commercially confidential.

- Permanent records are those which need to be retained in the archive for specified periods of time; there is some guidance on retention periods in section 2 below. Non-permanent documents are those that do not need to be archived for specific periods – examples of this would be drafts of documents, information that is used to construct other records, students work and a whole host of information used to support College activity – and which probably form the bulk of information held in departments. Departments should provide guidance to staff about how this material is stored and when it needs to be destroyed to meet departmental requirements.

- Material that is essentially the property of learners, including assignments, portfolios and artwork for display, should be returned to its owners immediately after it has been through the assessment and internal verification process; it does not constitute a record in the sense of this Policy. **Learners should be given notice at the end of their programme to collect any remaining material. Work not collected by this period will be destroyed in line with the College's destruction procedures.**

The flow chart and schedule in section 3 below provides guidance on how to manage the storage and destruction of documents in each category.

2. Retention periods for archived material

These guidelines are taken from a number of sources including but not limited to *Data Protection in the Education Sector, AoC*, JISC and CIPD.

Where electronic records are not able to be destroyed due to restrictions with the electronic systems, disproportionate workload involved in the destruction or the records, the records will either be archived, or access will be further restricted if possible. Management and destruction of electronic records shall be considered in the procurement of, development and upgrade of all systems.

Curriculum and learner records			**Notes**	**Responsibility**
Student Records	10 complete academic years		Limitation Act 1980	Head of MIS
Assessment marks	10 complete academic years			Head of MIS
Student personal and academic references	6 complete academic years	Recommended		Student Services
HE student examination scripts and records relating to assessment	5 years	Recommended		Assistant Principal - Adult & HE & Childcare & Healthcare
Coursework	In line with awarding organisation requirements or for a minimum of to the end of the academic year plus one full academic year (whichever is the greater).	Recommended		Assistant Principal - Quality and Standards/ Heads of Curriculum
Staff records - Director of HR				
Personnel files including staff development records and notes of disciplinary and grievance hearings	6 years from end of employment End of employment/ last action on case plus 6 years	Recommended	Provision of references and potential litigation	Director of HR
Application forms and interview notes	6 months from date of interview if unsuccessful Add to personnel file if successful	Recommended	Time limits on litigation	Director of HR
Facts relating to redundancy	6 years from last redundancy	Recommended	Limitation Act 1980	Director of HR
Health records	During employment	Required	MHSW Regulations	Director of HR

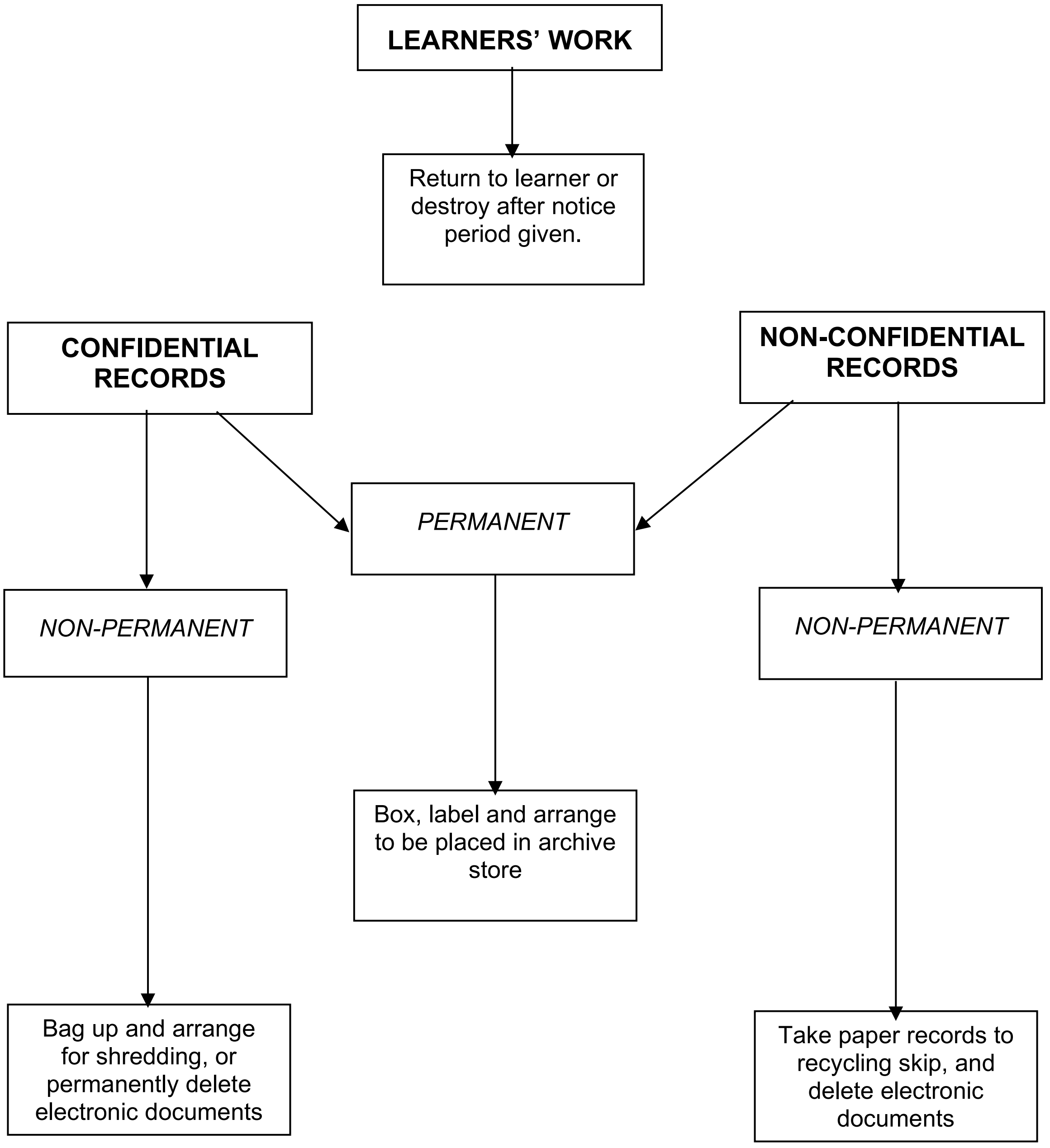
Health records where reason for termination of employment is connected with health, including stress related illness	3 years 12 years from end of employment	Recommended	Limitation period for personal injury claims	Director of HR
Medical records kept by reason of COSHH	40 years	Required	Control of Substances Hazardous to Health Regulations 2002 Control of Asbestos at work regulations 2002 Control of Lead at work regulations 2002	Director of HR
Statutory Sick Pay records and calculations	6 after the end of the financial year to which the records relate	Required	Income Tax (Employment Regulations) 1993	Director of HR
Statutory Maternity Pay records and calculations	3 years after the end of the financial year to which the records relate.	Required	Income Tax (Employment Regulations) 1993 Social Security contributions and benefits act 1992 Statutory maternity pay (general) regulations 1986 (amended 2005)	Director of HR
Wages and salary records	6 years	Required	Taxes Management Act 1970	Director of HR
Pension Contributions	12 years after benefit ceases			Director of HR
Income tax and National Insurance returns, including correspondence with tax office	3 years after the end of the financial year to which the records relate	Required	Income Tax (Employment Regulations) 1993	Director of HR
Health and Safety – Accident report	3 years following date of last entry	Required	Health and Safety at work Act 1974	Director of HR

Working time records	2 years from the date on which they were made	Required	The Working Time (amendment) Regulations 2003	Director of HR
Administrative records				
Financial records (detailed breakdown issued and kept in Finance Office)	6 years from end of financial year	Required	Financial Regulations	Head of Financial Services
Documentation relating to the implementation and financing of ESF projects	10 years after the programme ends or final payment has been made	Required	European Regulation 1260/1999	External Funding Manager Head of Financial Services
Documentation relating to ESF funded work (non-projects)	Records will be kept in line with timescales as determined by the funder	Recommended/ Required	As determined by Funder	External Funding Manager
Papers relating to Governors and Governor's meetings	Indefinitely	Recommended	To be able to retrieve information relating to major decisions affecting the College	Clerk to the Corporation
Meetings of Corporate and Senior Management teams	At least 5 years (all meeting papers held electronically).	Recommended	As above	Executive PA
Internal correspondence	2 years	Recommended	As above	All Heads of Areas
Circulars and reference publications	3 years unless relating to funding and finance issues		As above	All Heads of Areas
Records relating to leases, title deeds, insurance policies	Minimum of 40 years from date of issue	Requirement	Normal practice and financial regulations Employers' liability (compulsory insurance) regulations 1998	Head of Financial Services Head of Estates and Health & Safety

Information relating Governors and Senior Management	Indefinitely	Recommended	CIPD	Clerk to the Corporation Executive PA
Safeguarding records				
Safeguarding allegations against staff	person’s normal retirement age or for 10 years after the allegation — whichever is longer (unless found to be malicious/false when they should be removed unless consent given to retain).	Required	Keeping Children Safe in Education (KCSIE)	Director of HR
Safeguarding allegations against students	Until student turns 25.	Required	Keeping Children Safe in Education (KCSIE)	Assistant Principal Personal Development Vocational & Foundation

Electronic Records - Type of data	When will the College delete it (if electronic)	How will the College delete it (if electronic)?	Responsibility
Network Based Home Area (Staff)	6 Months after HR leave date	Script linked to HR System	Head of IT Services
Network Based Home Area (Fin, HR & CLT)	6 Months after HR leave date	Script linked to HR System	Head of IT Services
Emails	3 years (unless exempt – Finance, Pensions etc.)	Microsoft (Office 365) Data Retention Rule	Head of IT Services
Network Based Home Area (Students)	6 Months after leave date	Script marks for deletion, administrator clears manually.	Head of IT Services

3. Storage and destruction of records by departments


LEARNERS' WORK
Return to learner or destroy after notice period given.
CONFIDENTIAL RECORDS
NON-CONFIDENTIAL RECORDS
PERMANENT
NON-PERMANENT
NON-PERMANENT
Box, label and arrange to be placed in archive store
Bag up and arrange for shredding, or permanently delete electronic documents
Take paper records to recycling skip, and delete electronic documents

Retention and destruction schedule	By whom	By when
Classify all material held by curriculum and service area departments	Heads of Departments	Annually by the end of July
Box up permanent hard-copy records to be archived, and label with destruction date according to departmental guidelines	Heads of Departments	Annually by the end of August
Copy permanent electronic records to be archived to CD/DVD, label with destruction date and add to boxes of hard-copy archive material as above	Heads of Departments	Annually by the end of August
Collect labelled boxes of records for archive and remove to secure archive store	Customer Service Supervisor	Annually by the end of August
Write to learners informing them of the deadline for collection of academic work before it is destroyed	Course Team Leaders	End of Year + one term.
Move non-confidential, non-archive hard-copy material to paper skip	Heads of Departments	Weekly/monthly
Move confidential non-archive hard-copy material to bin bags	Heads of Departments	Weekly/monthly
Collect and shred bags of confidential documents	Customer Service Supervisor	Weekly
Electronically delete all transactional electronic records, i.e. those that are not to be archived and are not required for use	All	As required

4. Information security procedures

Each Curriculum Area/ Department should have annually reviewed procedures in place to:

- Provide appropriate physical and electronic security to prevent unauthorised access to relevant records (e.g. locked cupboards and filing cabinets, password protected files and shared network drives)

- Ensure that named individuals are responsible for all records held

- Ensure that requests for information (internally and externally) are dealt with appropriately, and passed to the Data Protection Officer where they relate to the Freedom of Information or Data Protection Policies

In addition:

- The Head of MIS should ensure that appropriate mechanisms are in place to prevent unauthorised access to electronic records and documents through MIS internal procedures and permissions. Similarly, the Head of IT Services should ensure there are appropriate mechanisms in place to present unauthorised access to system as outlined in the IT Security Policy.

- Physical Resources should ensure that the archive store is physically secure, and that there are mechanisms to provide access only to authorised individuals.

- The Head of MIS, in collaboration with the Head of IT Services, should ensure that the College Business Continuity Plan provides for appropriate back-up of relevant records.

- The College Induction Programmes for staff include should training on procedures governing access to, and the security of information, documents and records held by the College.