Name of Policy	**Data Retention Policy**
Purpose	This policy addresses the requirements surrounding Data Retention as set out by the Data Protection Act and how Macclesfield College meets its obligations by: • Minimising the retention periods of records whilst ensuring that the information needs of the business are met. • Ensuring that records required for legal and evidential purposes are kept for the appropriate period. • Ensuring that all records are not destroyed prematurely. • Ensuring all files are destroyed in a managed, secure & confidential manner with an audit trail.

Responsibility of / Job Title	Head of IT, MIS and Exams		
Equality Assessment By Whom	Head of IT, MIS and Exams	**Date**	08/2023
Version	3	**Date of next review (month and year)**	07/2025

		Date
Approved by	SMT	September 2023
	Corporation	October 2023

Related policies or procedures or parent policy if applicable	Data Protection Policy Information Security Policy
Groups/bodies consulted in the development of the policy	British Standard for Records Management (BS ISO 15489-2016) General Data Protection Regulation Data Protection Act 2018 Freedom of Information Act 2000 Environmental Information Regulations 2004 Macclesfield College Information Security Committee Jisc Records Retention Management
To be published on College website	Yes
To be published on Student Hub	No

Purpose

Macclesfield College must, in respect of its processing of personal and organisational data, comply with the Data Protection Act 2018 and related legislation (together, "Data Protection Laws").

The College has a responsibility to maintain its records and a legal obligation to only keep personal data for as long as it is required for its intended purpose.

The College should store its records in a secure manner in line with the Data Protection Policy, IT Security Policy and hold onto and dispose of records in line with the Data Retention Schedule section of this policy.

1. Scope

This policy applies to all College employees, consultants, contractors and temporary personnel hired to work on behalf of the College.

All College personnel must always comply with this policy. If you have any queries regarding this policy, please consult your line manager and/or the Data Protection Officer. You are advised that any breach of this policy will be treated seriously and may result in disciplinary action.

2. Responsibilities

The **Head of IT, MIS and Exams** is responsible for reviewing and enforcing this policy through the Information Security Committee.

The **Information Security Committee** are responsible for informing this policy ensuring their staff are kept up to date within their departments of this policy and the Data Retention Schedule.

Business Support Leads, Centre Principals and System Owners are responsible for ensuring that their departments act in compliance with this policy and the Data Retention Schedule.

The **Data Protection Officer** assists the College in monitoring internal compliance, inform and advise on the College's data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the Information Commissioner. The Data Protection Officer is responsible for auditing aspects of Data Retention, disposal, transfer and archives and any exceptions to these.

All **College Staff** will read and agree to this policy when they start at the College as well as being able to access the policy and the Data Retention Schedule through the Staff Intranet. This policy does not form part of any College personnel's contract of employment and the College reserves the right to change this policy at any time, giving employees at least one months' notice of any changes to the policy.

3. Data Retention Schedule

The College Data Retention Schedule documents the minimum retention periods for the College's hard copy and electronic records based on business needs and legal requirements. It has been written in line with JISC guidance on FE retention which can be accessed at: https://www.jisc.ac.uk/full-guide/records-retention-management

The Data Retention Schedule is accessible on the Staff Intranet and is split into the following retention schedules:

- A: ALS
- B: Data Protection
- C: Leadership
- D: Estates
- E: Examinations
- F: Finance
- G: Governance
- H: Human Resources
- I: IT Support
- J: Learner Experience
- K: Learning Resource Centre
- L: Marketing
- M: Maxim
- N: MIS
- O: Print Room
- P: Quality
- Q: Reporting
- R: Safeguarding
- S: Student Services
- T: Teaching

If any employee believes that a particular piece of personal/organisational data needs to be kept for more or less time than the period set out in this policy, the Data Protection Officer (DPO) should be informed for guidance. Any exceptions will be either documented by the DPO or be considered as part of the next policy review.

The College holds as Information Asset Register (IAR) which is regularly reviewed by the Information Security Committee, in compliance with the Data Protection Act. The IAR references retention periods for personal and special category data which are kept in line with the Data Retention Schedule.

4. Destruction of Data

Where records have been identified for destruction, they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, inquiries, complaints or grievances.
All paper records containing personal data, special category data or sensitive policy information should be placed in the sealed disposal bins ready for shredding. All electronic information will be deleted. Any electronic device containing data storage must be secure wiped by IT Support before disposal.

The College maintains a database of records which have been destroyed and who authorised their destruction.

When destroying documents, the appropriate staff member should record in this list at least the following information:

- File reference (or other unique identifier)
- File title/description
- Number of files

- Name of the authorising officer
- Date destroyed or deleted from system
- Data Retention Schedule item reference number that the data relates to (refer to the Data Retention Schedule)
- Person(s) who undertook destruction

5. Archiving of Data

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the Data Protection Officer. The appropriate staff member, when archiving documents should record in this list the following information:

- File reference (or other unique identifier)
- File title/description
- Number of files
- Name of the authorising officer
- Date archived
- Data Retention Schedule item reference number that the data relates to (refer to the Data Retention Schedule)
- Person(s) who undertook the archiving process

Archiving of data should be overseen and supervised by the Data Protection Officer.

6. Transfer of Data

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or secure cloud storage. The lifespan and accessibility of the media and the ability to migrate data where necessary should always be considered.

We retain the Learner’s educational record whilst the learner remains at the College. Once a learner leaves the College, their file will be sent securely to their next College. The responsibility for retention then shifts onto the next College. We will retain the file for one year following transfer in case any issues arise as a result of the transfer.

All data that is transferred b paper copy or electronic means must be done so securely (e.g. password-protected)

7. Data stored in Emails

Emails accounts should not be used as record keeping systems. Generally, emails may need to fall under different retention periods (for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a learner record). It is important to note that the retention period will depend on the content of the email and it is important that staff must file those emails / attachment in the relevant filing / electronic management systems to avoid the data becoming lost or inaccessible.

8. Safeguarding Records

Safeguarding records may be kept longer than the Data Retention Schedule as required by any inquiries taking place. At the conclusion of the inquiry, it is likely that an indication regarding the appropriate retention periods of the records will be made.

Please refer to the ‘Record Keeping’ section of the College’s Safeguarding Policy for more information.

9. Review and Monitoring

The relevance, efficacy and effectiveness of this Data Retention Policy will be reviewed in line with the cycle of strategic management activities to facilitate continuous improvement. The results of the review process will be analysed, and changes made to the policy where appropriate.