DATA RETENTION POLICY

Version	Approved by Southend City Council Finance, Curriculum and Quality Group	Reviewed
003	**December 2022**	**Annually**
Revisions: **Added specific entry for "Learner Records" to retention schedule**		

The College has a responsibility to maintain its records and record keeping systems. When doing this, the College will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the College's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the College from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The College may also vary any parts of this procedure, including any time limits, as appropriate in any case.

DATA PROTECTION

This policy sets out how long employment-related and learner data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the College. The College's Data Protection Policy outlines its duties and obligations under the UK GDPR.

RETENTION SCHEDULE

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the College will adhere to the standard retention times listed within that schedule.
Paper records will be regularly monitored by a data log.

Electronic records will be regularly monitored to see if it is still needed to be retained.

The schedule is a relatively lengthy document listing the many types of records used by the College and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

DESTRUCTION OF RECORDS

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, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

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: -

- File reference (or other unique identifier);
- File title/description;
- Number of files;
- Name of the authorising officer;
- Date destroyed or deleted from system; and
- Person(s) who undertook destruction.

RECORD KEEPING OF SAFEGUARDING

Any allegations made that are found to be malicious must not be part of the personnel records.

For any other allegations made, the College must keep a comprehensive summary of the allegation made, details of how the investigation was looked into and resolved and any decisions reached. This should be kept on the personnel files of the accused.

Any allegations made of sexual abuse should be preserved by the College for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse. All other records (for example, the personnel file of the accused) should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. Guidance from the Independent Inquiry Child Sexual Abuse states that prolonged retention of personal data at the request of an Inquiry would not contravene data protection regulation provided the information is restricted to that necessary to fulfil potential legal duties that the College may have in relation to an Inquiry.

Whilst the Independent Inquiry into Child Sexual Abuse is ongoing, it is an offence to destroy any records relating to it. At the conclusion of the Inquiry, it is likely that an indication regarding the appropriate retention periods of the records will be made.

ARCHIVING

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 each Department Head. 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; and
- Name of the authorising officer.

TRANSFERRING INFORMATION TO OTHER MEDIA

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 virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

TRANSFERRING INFORMATION TO ANOTHER COLLEGE

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

RESPONSIBILITY AND MONITORING

The GDPR Lead has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the College, is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to the GDPR Lead.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.
Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

EMAILS

Emails accounts are not a case management tool in itself. 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 file those emails in the relevant areas to avoid the data becoming lost.

LEARNER RECORDS

All Colleges with the exception of independent Colleges, are under a duty to maintain a learner record for each learner. If a learner changes Colleges, the responsibility for maintaining the learner record moves to the next College. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD
1. Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the College has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	6 years after employment ceases
Immigration checks	Two years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel, disciplinary and training records	While employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations: • Opt out forms • Records of compliance with WTR	• Two years from the date on which they were entered into

	• Two years after the relevant period
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.
2. Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to
Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	Until replaced/updated plus 3 years
3. Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
College Development Plans	3 years from the life of the plan
Visitors Book and Signing In Sheets	6 years
Newsletters and circulars to staff, parents and carers and learners	1 year (and the College may decide to archive one copy)
4. Health and Safety Records	
Health and Safety consultations	Permanently
Health and Safety Risk Assessments	Life of the risk assessment plus 3 years
Any records relating to any reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years provided that all records relating to the incident are held on personnel file

Fire precaution log books	6 years
Medical records and details of: - • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made
5. Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
6. Learner Records	
Details of whether admission is successful/unsuccessful	1 year from the date of admission/non-admission
Admissions register	Entries to be preserved for three years from date of entry
College Meals Registers	Current year plus 3 years
Free College Meals Registers	Current year plus 6 years
Learner Records (Name / Address / Course Details / Achievements / Disability Disclosures / Benefit Status etc.)	6 Years for end of financial year in which the funding was claimed to comply with auditing requirements.
Attendance Registers	6 years from the date of entry
Special Educational Needs files, reviews and individual education plans (this includes any statement and all advice and information shared regarding educational needs)	Until the learner turns 25.
Learner ILPs (Individual Learning Plan)	As long as they are a learner or 1 year following the receipt of result (or outcome of appeal)
ASDAN: 1. Registration records	5 years following registration

2. Ongoing records of learner's formative and summative achievements 3. Records of final results and details of certification for registered learners 4. Portfolio of evidence 5. Samples of learners work for monitoring and standardisation	1 year following the receipt of result (or outcome of appeal) 3 years following registration No longer than 6 months after moderation Up to 3 years with written agreement
7. Emails	3 years
8. CCTV	Within 30 days
9. Test and Trace	After 21 Days

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174