



Records Management and Data Retention Policy

Higher Education · Performing Arts
Validated by the University of West London

Approved: August 2026

Document Control

Policy Title	Records Management and Data Retention Policy
Institution Name	Triple Threat Training Limited (trading as GAMTA)
Policy Category	Information Governance and Data Protection
Approval Authority	Academic Board
Validating Partner	University of West London
Applicable Provision	All records created or held across GAMTA provision, including validated Higher Education (University of West London) and HNC provision (SQA, GPRO Scotland)
External Regulatory Alignment	UK GDPR; Data Protection Act 2018; Freedom of Information (Scotland) Act 2002 (where applicable); Public Records (Scotland) Act 2011; Equality Act 2010
Document Status	Approved Institutional Policy
Approved	August 2026

Contents

TRIPLE THREAT COLLEGE

RECORDS MANAGEMENT AND DATA RETENTION POLICY

Policy Information and Document Control

1. Introduction

1.1 For the purpose of this Policy, Triple Threat Training Limited, trading as GAMTA, shall hereafter be referred to as “the College”.

1.2 Effective records management is essential to the efficient operation of the College, the protection of the rights of students, staff, and other members of the College community, and the discharge of the College’s legal, regulatory, and contractual obligations.

1.3 The College is committed to establishing and maintaining good records management practice, ensuring that records of evidential, legal, regulatory, historical, academic, or business importance are retained for the periods necessary to support those purposes, while ensuring that records which are no longer required are securely disposed of in accordance with applicable law.

1.4 Robust records management supports the College in meeting its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information (Scotland) Act 2002 (where applicable), the Environmental Information (Scotland) Regulations 2004 (where applicable), UKVI sponsor licence duties, and the academic and quality assurance expectations of the validating partner and relevant Scottish awarding bodies.

1.5 This Policy supplements the College’s Data Protection Policy, Information Security Policy, Acceptable Use of IT Policy, CCTV Policy, and the Privacy Notices issued by the College, and shall be read in conjunction with those documents.

1.6 This Policy applies across all College provision, including validated higher education programmes delivered in partnership with the validating partner, HNC and HND provision delivered in partnership with relevant Scottish awarding bodies, and further specialist programmes within dance, singing, acting, musical theatre, and wider performance-based education.

2. Purpose of the Policy

2.1 The purpose of this Policy is to establish a clear, consistent, and proportionate framework for the creation, management, classification, retention, secure storage, access, and disposal of records held by the College, in any format.

2.2 This Policy seeks to ensure that records of evidential, legal, regulatory, historical, academic, or business importance are identified, retained for appropriate periods, and accessible when required, while records that are no longer required are disposed of securely and in accordance with applicable law.

2.3 This Policy seeks to support compliance with the College’s legal and regulatory obligations, including those under the UK GDPR, the Data Protection Act 2018, the Freedom of Information (Scotland) Act 2002 (where applicable), and the academic and quality assurance expectations of the validating partner and relevant Scottish awarding bodies.

2.4 This Policy seeks to support efficient working practices, enable timely retrieval of records, prevent the unnecessary duplication or premature destruction of records, and contribute to the security and integrity of College information.

3. Scope

3.1 This Policy applies to all information and records created, received, or held by the College in the course of its activities, regardless of format. This includes paper, electronic, audio, video, photographic, digital, and online records.

3.2 This Policy applies to all members of the College community who create, receive, or use records, including academic, professional, technical, and production staff, governors, students where applicable, contractors, suppliers, and external partners acting on behalf of the College.

3.3 This Policy applies to records relating to students, applicants, staff, governors, contractors, suppliers, partner institutions (including the validating partner and relevant Scottish awarding bodies), placement providers, audiences, visitors, and research participants, where applicable.

3.4 This Policy applies to records arising from rehearsal, studio, technical, production, and performance activity, including recordings, photographs, design materials, scripts, choreography notation, performance archives, and audition records, having regard to relevant intellectual property and consent arrangements.

3.5 This Policy operates alongside related institutional policies including the Data Protection Policy, the Information Security Policy, the CCTV Policy, the Acceptable Use of IT Policy, the Admissions Policy, the Student Terms and Conditions, the Student Charter, the Student Code of Conduct and Disciplinary Regulations, the Attendance, Engagement, Interruption, Withdrawal and Termination Policy, the Complaints Policy and Procedure, the Academic Appeals Regulations, the Fitness to Study Policy, the Harassment and Sexual Misconduct Policy, the Equality, Diversity and Inclusion Policy, the Code of Practice on Freedom of Speech and Academic Freedom, the Reasonable Adjustments and Inclusive Learning Support Policy, the Fair Access to Assessment Policy, the Extensions, Mitigation, Deferral and Withdrawal Policy, and the Safeguarding Policy.

4. Legal and Regulatory Framework

4.1 This Policy has been developed having regard to the following legal and regulatory frameworks:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Freedom of Information (Scotland) Act 2002 (FOISA), where applicable to the College's status;
- Environmental Information (Scotland) Regulations 2004 (EIRs), where applicable;
- Public Records (Scotland) Act 2011, where applicable;
- Privacy and Electronic Communications Regulations 2003 (PECR);
- Equality Act 2010;
- Prescription and Limitation (Scotland) Act 1973, and where relevant the Limitation Act 1980, in respect of retention periods supporting the limitation of legal action;
- UKVI Student Sponsor Licence record-keeping duties applicable to international students sponsored under the UKVI Student Route;
- HMRC and Companies House record-keeping requirements, where applicable;
- Student Awards Agency Scotland (SAAS) and Scottish Funding Council reporting and record-keeping requirements, where applicable;
- Information Commissioner's Office (ICO) Codes of Practice and guidance;
- ISO 15489 Records Management Principles;

- Validating partner and relevant Scottish awarding body record-keeping expectations in respect of academic standards, quality assurance, student progression, and award arrangements.

4.2 Where a member of the College community is uncertain as to the application of any legal or regulatory requirement to a particular record or category of records, advice shall be sought from the Information Governance Lead, the Data Protection Officer, or such other officer as the College may designate.

5. Definitions

5.1 “Record” means information created, received, and maintained as evidence and information by the College or a member of its community in pursuance of legal, regulatory, or contractual obligations, or in the transaction of business, in accordance with ISO 15489. Records may be held in any format, including paper, electronic, email, audio, video, photographic, or digital form.

5.2 “Personal Data” has the meaning given to it under the UK GDPR, namely any information relating to an identified or identifiable natural person.

5.3 “Special Category Data” has the meaning given to it under Article 9 of the UK GDPR, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health, or data concerning a person’s sex life or sexual orientation.

5.4 “Records Owner” means the senior officer of the College with overall responsibility for a defined class of records, as identified in Appendix C.

5.5 “Information Governance Lead” means the senior officer of the College designated to oversee the operation of this Policy and related information governance matters. The College may designate the same officer as Data Protection Officer where appropriate.

5.6 “Data Protection Officer” means the officer of the College responsible for monitoring compliance with the UK GDPR and the Data Protection Act 2018, where the College is required to appoint a Data Protection Officer or has elected to do so.

5.7 “Retention Period” means the period of time for which a record is to be retained before review or disposal, in accordance with this Policy and the Records Retention Schedule at Appendix B.

5.8 “Information Classification” means the categorisation of records by sensitivity in accordance with the framework set out at Appendix A.

5.9 “Secure Disposal” means the disposal of records, in any format, by methods which prevent unauthorised retrieval or reconstruction, in accordance with Appendix D.

6. Underpinning Principles

6.1 Records (the “Six Rs”). The College shall manage records in accordance with the following principles:

- Records – records are evidence of the College’s actions and decisions and shall be retained for as long as required by legal, regulatory, contractual, or business need;
- Responsibility – all staff and other members of the College community have responsibility for records and shall be aware of records they create, receive, and hold;
- Risk – the College shall manage risks arising from loss, damage, unauthorised access, or loss of control of records;
- Retention – records shall be retained only for as long as needed;

- Rights – students, staff, and other data subjects have rights in respect of their personal data under the UK GDPR and the Data Protection Act 2018, and members of the public may, where applicable, have rights of access to information held by the College under the Freedom of Information (Scotland) Act 2002 or the Environmental Information (Scotland) Regulations 2004;
- Reliability – records shall be managed in a manner that ensures their authenticity, integrity, accuracy, and usability.

6.2 Data Protection Principles. Personal data held in College records shall be processed in accordance with the principles set out in Article 5 of the UK GDPR, namely:

- lawfulness, fairness, and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security);
- accountability.

6.3 Proportionality. Retention periods shall be proportionate to the purposes for which the records were created and the legal, regulatory, contractual, or business needs they support.

6.4 Single Copy Principle. Multiple copies of the same record shall not be retained unnecessarily. Where duplicate copies exist, only one authoritative version shall be retained, with extraneous copies disposed of securely where appropriate.

6.5 Format Neutrality. Retention periods shall apply equally to all formats of a record, including paper, electronic, email, audio, video, photographic, and digital records.

6.6 Accessibility. Records shall be managed in a manner that supports timely access, retrieval, and use for legitimate purposes, including in response to data subject requests and lawful information requests.

6.7 Security. Records shall be managed with appropriate technical and organisational measures to protect against unauthorised access, alteration, loss, or disclosure, in accordance with the Information Security Policy and the Information Classification Framework at Appendix A.

7. Records and Their Management

7.1 Records are an essential resource of the College, providing evidence of decisions, actions, transactions, and the discharge of legal, regulatory, contractual, and academic obligations. Records may include, but are not limited to:

- student records (applications, enrolment, assessment, attendance, support, mitigation, complaints, appeals, conduct, withdrawals, awards);
- staff records (recruitment, employment, performance, payroll, training, disciplinary);
- governance records (Board and committee papers, minutes, decisions, policies);
- academic and quality assurance records (programme approval, validation, monitoring, External Examiner reports, audit material);
- financial records (income, expenditure, tuition fees, contracts, payroll, tax);
- operational records (timetables, room bookings, health and safety, incident reports, safeguarding);

- rehearsal, studio, production, and performance records (rehearsal schedules, casting decisions, choreography notation, scripts, designs, audition records, performance recordings, photographic records);
- placement records (placement provider agreements, evaluations, monitoring information);
- partnership records (validating partner correspondence, awarding body records, sub-contracted provision records);
- communications records (emails, correspondence, meeting notes, internal memos);
- system and technical records (access logs, system audit trails, backup records).

7.2 All records, regardless of format, shall be managed in accordance with this Policy and the Records Retention Schedule at Appendix B.

8. Information Classification

8.1 The College classifies its records into the categories set out at Appendix A, namely Public, Internal, Confidential, and Strictly Confidential. The classification of a record determines the protection, access, and handling arrangements applicable to it.

8.2 Records shall be classified at the point of creation or receipt, having regard to the sensitivity of the content, the categories of data subject involved, and the risk arising from unauthorised disclosure.

8.3 Records classified as Confidential or Strictly Confidential shall be handled in accordance with the Information Security Policy, including appropriate access controls, encryption where required, and secure disposal.

8.4 Special Category Data shall normally be classified as Strictly Confidential and shall be processed only where one of the conditions set out in Article 9 of the UK GDPR is met.

9. Records Retention Schedule

9.1 The College maintains a Records Retention Schedule, set out at Appendix B, which establishes the retention periods applicable to defined classes of records held by the College.

9.2 The Schedule is intended to:

- improve efficiency of working practices and enable timely retrieval of records;
- prevent records from being discarded prematurely;
- ensure that records are not retained for longer than necessary;
- eliminate the retention of unnecessary duplicate records;
- provide a consistent and controlled framework for the disposal of records across the College;
- support compliance with the UK GDPR, the Data Protection Act 2018, the Freedom of Information (Scotland) Act 2002 (where applicable), and other relevant frameworks;
- support the College's academic, quality assurance, and validating partner obligations.

9.3 The Schedule is organised by class of record. For each class, the Schedule sets out the type of record, the retention period, the Records Owner, the information classification, and the justification for the retention period.

9.4 Retention periods are independent of format and apply equally to paper and electronic records.

9.5 Where a particular record does not fall within the categories set out in the Schedule, the relevant Records Owner shall seek advice from the Information Governance Lead or the Data Protection Officer.

9.6 The Records Retention Schedule shall be reviewed annually and updated where required by legislative, regulatory, operational, or validating partner changes.

10. Creation, Capture, and Storage of Records

10.1 Records shall be created in a manner that captures sufficient information to support the decisions, actions, and transactions to which they relate, having regard to the principles of accuracy, completeness, and reliability.

10.2 Records shall be stored in approved College systems or locations, with appropriate access controls. Personal data and Confidential or Strictly Confidential records shall not be stored on unauthorised personal devices, personal email accounts, unapproved cloud storage, or external media without the prior approval of the Information Governance Lead or the Data Protection Officer.

10.3 Email correspondence may constitute a record where it provides evidence of decisions, actions, transactions, or communications relevant to the College. Members of staff shall identify which emails constitute key records and shall retain them in accordance with this Policy, while routinely deleting transitory or duplicative correspondence.

10.4 Where records are held on external systems, including those operated by the validating partner, awarding bodies, placement providers, or contracted suppliers, appropriate data sharing and processing arrangements shall be in place, in accordance with the UK GDPR and the College's Data Protection Policy.

11. Access to Records

11.1 Access to records shall be granted on a need-to-know basis, in accordance with the Information Classification Framework at Appendix A and the Information Security Policy.

11.2 Data subjects, including students, staff, applicants, and other individuals, have rights in respect of their personal data under the UK GDPR and the Data Protection Act 2018, including the right of access, the right to rectification, the right to erasure where applicable, the right to restriction of processing, the right to object, and the right to data portability where applicable.

11.3 Subject access requests shall be considered in accordance with the College's Data Protection Policy and applicable timescales under the UK GDPR.

11.4 Where the College is subject to the Freedom of Information (Scotland) Act 2002 or the Environmental Information (Scotland) Regulations 2004, requests for information shall be considered in accordance with the applicable framework.

11.5 Records may be disclosed to the validating partner, awarding bodies, regulatory authorities, UK Visas and Immigration, placement providers, funding bodies including SAAS, and other authorised parties where reasonably necessary for the discharge of the College's legal, regulatory, contractual, or academic obligations, in accordance with the College's Privacy Notices.

12. Disposal of Records

12.1 Records that have reached the end of their retention period shall be disposed of in accordance with the Schedule, unless a specific reason exists for further retention (such as an ongoing investigation, dispute, regulatory matter, or legal claim).

12.2 Records shall be disposed of in a manner appropriate to their classification, having regard to the secure disposal methods set out at Appendix D.

12.3 Confidential and Strictly Confidential records shall be disposed of using secure methods, including confidential waste services, secure shredding, certified data destruction services for electronic media, and verified deletion from electronic systems.

12.4 A record of significant disposal activity, particularly in respect of categories of records subject to specific regulatory requirements, shall be maintained where required.

12.5 Where records are subject to a litigation hold, regulatory request, investigation, or ongoing matter, disposal shall be suspended pending resolution of the matter.

13. Records Relating to Specific Categories

13.1 Student Records

13.1.1 Student records shall be maintained in accordance with this Policy, the Student Privacy Notice, and the academic regulations of the validating partner or relevant awarding body.

13.1.2 Records of academic award, including transcripts and certification information, shall normally be retained on a permanent basis, having regard to the College's and the validating partner's award verification obligations.

13.1.3 Records of disciplinary or fitness-to-study matters shall be retained for the period set out in the Schedule, with summary retention where appropriate to support reference requests and regulatory disclosures.

13.2 Staff Records

13.2.1 Staff records shall be maintained in accordance with the Staff Privacy Notice and applicable employment law requirements.

13.3 UKVI Student Sponsor Licence Records

13.3.1 Where the College sponsors international students under the UKVI Student Route, records required by UKVI sponsorship duties, including attendance, engagement, contact details, and right-to-study evidence, shall be retained for the period required by UKVI guidance, which is normally one year following the student ceasing to study, or such longer period as may be specified by UKVI.

13.4 Validating Partner and Awarding Body Records

13.4.1 Records relating to validated higher education provision delivered in partnership with the validating partner, and to HNC and HND provision delivered with relevant Scottish awarding bodies, shall be retained in accordance with the academic regulations and quality assurance expectations of the relevant partner.

13.4.2 Records of External Examiner reports, programme monitoring, validation events, periodic review, and re-approval shall be retained for the periods set out in the Schedule.

13.5 Rehearsal, Studio, Production, and Performance Records

13.5.1 Records arising from rehearsal, studio, production, and performance activity, including audition records, casting decisions, choreography notation, scripts, designs, performance recordings, and photographic records, shall be retained in accordance with the Schedule, having regard to the intellectual property arrangements set out in the Student Terms and Conditions and the consent arrangements applicable to recordings, photographs, and broadcast material.

13.5.2 Performance recordings used for assessment shall be retained for the period required by the validating partner or relevant awarding body.

13.6 Safeguarding Records

13.6.1 Safeguarding records shall be retained securely and confidentially in accordance with the Safeguarding Policy and applicable Scottish safeguarding guidance, having regard to the sensitivity of the information and the need to support any future safeguarding considerations.

14. Data Breaches and Incident Response

14.1 Where a personal data breach occurs, or is suspected, the matter shall be reported promptly to the Data Protection Officer or Information Governance Lead, in accordance with the Data Protection Policy and the Information Security Policy.

14.2 Personal data breaches shall be assessed, and where appropriate notified to the Information Commissioner's Office (ICO) within seventy-two (72) hours of the College becoming aware of the breach, in accordance with Article 33 of the UK GDPR.

14.3 Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, the College shall notify those individuals without undue delay, in accordance with Article 34 of the UK GDPR.

14.4 Records of personal data breaches shall be maintained in accordance with Article 33(5) of the UK GDPR, regardless of whether the breach is reportable to the ICO.

15. Training and Awareness

15.1 All staff and other members of the College community with records management responsibilities shall undertake training appropriate to their role, including induction on data protection, records management, and information security.

15.2 Staff in specialist roles, including the Information Governance Lead, the Data Protection Officer, Records Owners, and staff handling Strictly Confidential records, shall receive enhanced training appropriate to their responsibilities.

15.3 Training shall be refreshed at appropriate intervals and following any material change in legislation, regulatory guidance, or institutional practice.

16. Equality, Diversity and Inclusion

16.1 This Policy shall be operated in accordance with the principles of equality, diversity, accessibility, dignity, and inclusive participation, as set out in the Equality, Diversity and Inclusion Policy and the Equality Act 2010.

16.2 Records containing data relating to persons sharing protected characteristics, including Special Category Data, shall be handled with particular care and shall be processed only where one of the conditions set out in Article 9 of the UK GDPR is met.

16.3 Reasonable adjustments shall be considered in respect of access to records, including the provision of accessible formats where appropriate, in accordance with the Reasonable Adjustments and Inclusive Learning Support Policy.

17. Roles and Responsibilities

17.1 The Unibridge Group Board, or such other governing body as the College may designate, holds overall responsibility for the College's information governance arrangements, including this Policy.

17.2 The College Principal is responsible for the implementation of this Policy across the College.

17.3 The Information Governance Lead, and where appointed the Data Protection Officer, are responsible for the operational implementation of this Policy, including the maintenance of the Records Retention Schedule, the provision of advice and guidance, the management of data breach incidents, and reporting to the Unibridge Group Board and the Academic Quality and Student Support Committee.

17.4 Heads of Department, Course Leaders, and other senior officers are responsible for the management of records generated by activities within their areas, including ensuring that records are properly maintained, accessed only as authorised, and disposed of in accordance with the Schedule.

17.5 Records Owners, as identified in Appendix C, are responsible for the implementation of this Policy in respect of their assigned classes of records, including the identification of records, the application of retention periods, the management of information classification, and the secure disposal of records.

17.6 All staff who create, receive, or use records have records management responsibilities. Staff shall be aware of records they create and shall ensure that records are secured, retained, and disposed of in accordance with this Policy.

17.7 Staff are responsible for identifying which emails and other digital communications constitute records and managing them accordingly. Routine, transitory, or duplicative communications shall not be retained unnecessarily.

17.8 Students are responsible for engaging appropriately with the College's records management arrangements, including providing accurate information, complying with consent arrangements applicable to rehearsal, studio, production, and performance records, and complying with the Acceptable Use of IT Policy.

18. Monitoring, Review and Continuous Improvement

18.1 Compliance with this Policy shall be monitored by the Information Governance Lead, the Data Protection Officer where appointed, and the Academic Quality and Student Support Committee, with reporting to the Academic Board and the Unibridge Group Board.

18.2 Monitoring data shall include data breach reports, subject access request performance, retention schedule compliance, and outcomes of any audit activity.

18.3 This Policy and the Records Retention Schedule shall be reviewed annually, or earlier where required by legislative, regulatory, operational, or validating partner changes.

18.4 Review of this Policy shall take account of sector good practice, ICO guidance, validating partner expectations, and feedback from members of the College community.

19. Related Policies and Procedures

19.1 This Policy operates alongside the following related College policies and procedures:

- Data Protection Policy;
- Information Security Policy;
- Acceptable Use of IT Policy;
- CCTV Policy;
- Student Privacy Notice, Staff Privacy Notice, Applicant Privacy Notice, and other applicable Privacy Notices;
- Admissions Policy;
- Student Terms and Conditions;

- Student Charter;
- Student Code of Conduct and Student Disciplinary Regulations;
- Attendance, Engagement, Interruption, Withdrawal and Termination Policy;
- Complaints Policy and Procedure;
- Academic Appeals Regulations;
- Fitness to Study Policy;
- Harassment and Sexual Misconduct Policy;
- Equality, Diversity and Inclusion Policy;
- Code of Practice on Freedom of Speech and Academic Freedom;
- Reasonable Adjustments and Inclusive Learning Support Policy;
- Fair Access to Assessment Policy;
- Extensions, Mitigation, Deferral and Withdrawal Policy;
- Safeguarding Policy.

20. Approval and Version Control

20.1 This Policy has been approved through the College's academic governance arrangements and shall be reviewed in accordance with the published Policy Review Cycle.

20.2 Material amendments shall be considered and approved by the Academic Board or Unibridge Group Board as appropriate, with notification to the validating partner where appropriate.

20.3 Historic versions of this Policy and earlier versions of the Records Retention Schedule shall be retained in accordance with the principles set out in this Policy.

Appendix A – Information Classification Framework

The following classification framework shall be applied to records held by the College. Examples are illustrative and not exhaustive.

A.1 Public

A.1.1 Risk and Access: No or minimal risk. Information which the College has chosen to put into the public domain.

A.1.2 Examples: Prospectus, programme information, open day materials, opening times, published research, vacancy details, public-facing staff directory entries, College policies published on the website, audition information for public performances.

A.2 Internal

A.2.1 Risk and Access: Low risk. Information for which there is no significant risk in limited disclosure but which is not intended for wide circulation. Normally accessed by members of staff.

A.2.2 Examples: Internal emails, routine meeting minutes, internal communications, draft documents, internal operational schedules.

A.3 Confidential

A.3.1 Risk and Access: Medium to high risk. Inappropriate disclosure could cause reputational damage and breach contractual or legal obligations. Accessible only to those who need to access the information as part of their role.

A.3.2 Examples: Documents containing personal data, employee and student records, casting decisions, audition records, sensitive business data, financial records, programme monitoring papers, complaints and appeals papers (subject to data protection considerations).

A.4 Strictly Confidential

A.4.1 Risk and Access: Very high risk. Inappropriate disclosure could result in significant reputational damage, regulatory fines, breach of contract, and breach of other legal obligations. Accessible only to those who need to access the information as part of their role. Personal data should normally be encrypted in transit and at rest.

A.4.2 Examples: Special Category Data including medical, disability, and ethnicity data; safeguarding records; data relating to criminal convictions; business-critical information; College banking information; investigation records relating to harassment or sexual misconduct; sensitive UKVI compliance records.

Appendix B – Indicative Records Retention Schedule

The following indicative Records Retention Schedule sets out the retention periods applicable to defined classes of records held by the College. The Schedule shall be reviewed and updated annually. Specific retention periods may be varied by reference to the requirements of the validating partner, relevant Scottish awarding bodies, UKVI, SAAS, HMRC, or other regulatory authorities. Where a record does not fall within the categories set out below, advice shall be sought from the Information Governance Lead.

B.1 Recruitment and Admissions Records

B.2 Student Academic Records

B.3 Student Conduct, Complaints, and Fitness Records

B.4 UKVI Sponsorship Records

B.5 Staff Records

B.6 Governance and Strategic Records

B.7 Financial Records

B.8 Operational, Performance, and Production Records

B.9 IT and System Records

Appendix C – Records Owners and Responsibilities

The following framework identifies the principal Records Owners within the College. Where the College has not yet appointed an officer to a designated role, responsibility shall sit with the College Principal until such time as the appointment is made.

C.1 College Principal – overall accountability for the implementation of this Policy and ownership of governance records.

C.2 Information Governance Lead / Data Protection Officer – operational ownership of the records management framework, the Records Retention Schedule, data protection compliance, and data breach response.

C.3 College Registry – ownership of student academic records, attendance records, transcripts and awards, and academic appeals.

C.4 Head of Admissions – ownership of applicant and admissions records, audition records, and outreach data.

C.5 Academic Quality – ownership of programme approval, validation, monitoring, and External Examiner records.

C.6 Student Support Services – ownership of reasonable adjustments records, wellbeing and pastoral records, and Fitness to Study records.

C.7 Designated Safeguarding Lead – ownership of safeguarding records, harassment and sexual misconduct investigation records.

C.8 Human Resources – ownership of staff records, recruitment, employment, and HR-related disciplinary records.

C.9 Finance – ownership of financial records, tuition fee records, contracts, and funding body records.

C.10 IT Services – ownership of system access logs, backup records, and technical records.

C.11 UKVI Compliance Lead – ownership of UKVI sponsorship records, including CAS records and attendance records for sponsored students.

C.12 Head of Production – ownership of production records, scripts, design materials, and performance recordings.

Appendix D – Secure Disposal Methods

Records shall be disposed of in accordance with the methods set out below, having regard to the format of the record and its classification.

D.1 Paper Records – Public records may be disposed of through normal recycling. Internal records shall be disposed of through general recycling unless they contain identifying information. Confidential and Strictly Confidential records shall be disposed of through cross-cut shredding or a certified confidential waste service.

D.2 Electronic Records – Public and Internal records shall be deleted from active systems and backup retention shall be in accordance with the IT backup schedule. Confidential records shall be securely deleted from active systems. Strictly Confidential records and Special Category Data shall be securely deleted using approved methods, with documented evidence of destruction where required.

D.3 Removable Media and Hardware – End-of-life storage media and devices containing personal data shall be securely destroyed using certified data destruction services.

D.4 Audio and Video Recordings – Recordings containing personal data shall be securely deleted at the end of the applicable retention period. Where recordings have been consented to for archive purposes, retention shall be in accordance with the consent given.

D.5 Suspension of Disposal – Disposal shall be suspended where records are subject to a litigation hold, regulatory request, investigation, freedom of information request, subject access request, or other ongoing matter requiring retention.

Appendix E – Records Management Lifecycle

The records management lifecycle adopted by the College consists of the following stages.

E.1 Stage One – Creation or Receipt. Records are created or received in the course of College business and are classified in accordance with Appendix A.

E.2 Stage Two – Capture and Storage. Records are stored in approved College systems or locations with appropriate access controls.

E.3 Stage Three – Use and Access. Records are accessed and used on a need-to-know basis, in accordance with the Information Security Policy and the Data Protection Policy.

E.4 Stage Four – Maintenance. Records are maintained for accuracy, integrity, and usability throughout their retention period.

E.5 Stage Five – Review. At the end of the retention period set out in Appendix B, records are reviewed by the relevant Records Owner.

E.6 Stage Six – Disposal or Permanent Retention. Records are either securely disposed of in accordance with Appendix D or, where appropriate, retained permanently or for an extended period where required by legal, regulatory, historical, or academic considerations.

E.7 Stage Seven – Documentation. Significant disposal activity is documented where required, and the Records Retention Schedule is updated where necessary.

END OF POLICY