Privacy and Information Security Policy

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

Approved: August 2026

Document Control

Policy Title	Privacy and Information Security Policy
Institution Name	Triple Threat Training Limited (trading as GAMTA)
Policy Category	Data Protection and Information Security
Approval Authority	Academic Board
Validating Partner	University of West London
Applicable Provision	All personal data and information assets processed 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; Privacy and Electronic Communications Regulations 2003; NCSC good practice; Equality Act 2010
Document Status	Approved Institutional Policy
Approved	August 2026

Contents

TRIPLE THREAT COLLEGE

PRIVACY AND INFORMATION SECURITY POLICY

Incorporating the Applicant Privacy Notice (Schedule 1) and the Student Privacy Notice (Schedule 2)

1. Introduction

1.1 Triple Threat Training Limited, trading as GAMTA (the "College") is committed to the lawful, fair, transparent, and secure handling of personal data and to the protection of its information systems and the information held within them. This Policy sets out the College's framework for data protection and information security, and incorporates the Applicant Privacy Notice (Schedule 1) and the Student Privacy Notice (Schedule 2).

1.2 The College acts as a data controller in respect of personal data it processes about applicants, students, staff, governors, visiting practitioners, contractors, placement providers, visitors, and other individuals it interacts with in the course of its activities.

1.3 Performing arts education involves the creation of personal data unique to the sector, including casting and audition records, rehearsal and production notes, photographs and audio-visual recordings of rehearsals and performances, technical and production files, and records of physical contact protocols and intimacy arrangements. This Policy applies to such records as it does to all other categories of personal data.

1.4 The College is established in Scotland and applies this Policy in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and, where applicable, the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.

2. Purpose and Scope

2.1 The purpose of this Policy is to:

- ensure compliance with the UK GDPR, the Data Protection Act 2018, and related legislation;
- provide clear privacy information to applicants and students through the schedules to this Policy;
- set out the College's arrangements for information security, including technical and organisational measures;
- clarify the responsibilities of governors, staff, students, and third parties in handling personal data and using College information systems;
- establish arrangements for the management of personal data breaches and the exercise of data subject rights.

2.2 This Policy applies to all personal data processed by the College, regardless of format, and to all members of the College community who create, receive, use, or transmit personal data or who access College information systems. It applies on College premises, in remote working contexts, on College-managed devices and personal devices used for College purposes, and in cloud-hosted or third-party-operated systems used on the College's behalf.

3. Data Protection Principles

3.1 The College shall process personal data in accordance with the principles set out in Article 5 of the UK GDPR:

- Lawfulness, fairness, and transparency. Personal data shall be processed lawfully, fairly, and in a transparent manner, with clear privacy information provided to data subjects.
- Purpose limitation. Personal data shall be collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.
- Data minimisation. Personal data shall be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- Accuracy. Personal data shall be accurate and, where necessary, kept up to date, with reasonable steps taken to correct inaccuracies.
- Storage limitation. Personal data shall be kept in an identifiable form for no longer than is necessary, in accordance with the Records Management and Data Retention Policy.
- Integrity and confidentiality. Personal data shall be processed in a manner that ensures appropriate security, using appropriate technical and organisational measures.

3.2 The College, as data controller, is accountable for compliance with these principles and shall be able to demonstrate compliance, in accordance with Article 5(2) of the UK GDPR.

4. Lawful Bases for Processing

4.1 The College shall process personal data only where one or more of the lawful bases set out in Article 6 of the UK GDPR applies, and shall identify the applicable basis for each processing activity. The principal lawful bases on which the College relies are:

- Contract – performance of the educational contract with the student, and steps taken at the request of an applicant prior to entering into a contract;
- Legal obligation – compliance with statutory duties, including those under the Equality Act 2010, the Counter-Terrorism and Security Act 2015 (Prevent), UKVI sponsorship duties, employment law, and safeguarding legislation;
- Vital interests – protection of the vital interests of the data subject or another person, including in safeguarding and emergency situations;
- Public task – performance of a task carried out in the public interest in respect of higher and further education;
- Legitimate interests – pursuit of the College's or a third party's legitimate interests where not overridden by the rights of the data subject;
- Consent – where the College has obtained the data subject's clear, specific, and informed consent for a particular processing activity, including for marketing communications and for certain uses of images and recordings.

4.2 Where the College processes Special Category Data, including data revealing racial or ethnic origin, religious or philosophical beliefs, trade union membership, health data, sex life or sexual orientation, biometric data, or genetic data, the College shall identify an applicable condition under Article 9 of the UK GDPR and, where required, a condition under Schedule 1 to the Data Protection Act 2018. Special Category Data shall be processed with enhanced safeguards.

4.3 Where the College processes personal data relating to criminal convictions or offences, including data obtained through Disclosure Scotland or the Protecting Vulnerable Groups (PVG) Scheme, the College shall identify an applicable condition under Article 10 of the UK GDPR and Schedule 1 to the Data Protection Act 2018.

5. Data Subject Rights

5.1 Data subjects have the following rights under the UK GDPR, subject to applicable conditions and exemptions:

- the right to be informed about the processing of their personal data, through the Privacy Notices at Schedules 1 and 2 and similar notices issued to other data subjects;
- the right of access to their personal data and supporting information (a Subject Access Request);
- the right to rectification of inaccurate or incomplete personal data;
- the right to erasure (the right to be forgotten), in limited circumstances;
- the right to restriction of processing, in limited circumstances;
- the right to data portability, in limited circumstances;
- the right to object to processing, including direct marketing;
- rights in relation to automated decision-making and profiling.

5.2 Requests to exercise data subject rights should be addressed to the Information Governance Lead at the College's contact address. The College shall respond within one (1) calendar month of receipt of the request, extendable by up to a further two (2) months where the request is complex or numerous. No fee shall normally be charged, save where a request is manifestly unfounded or excessive.

5.3 Where the College cannot identify the requester, the College may seek proof of identity before responding.

6. Disclosure and Sharing of Personal Data

6.1 The College shall share personal data only where there is a lawful basis to do so. The principal categories of recipient are set out in the Privacy Notices at Schedules 1 and 2 and the Operational Records of Processing Schedule. They include:

- the validating partner, in respect of validated higher education provision;
- relevant Scottish awarding bodies, including the Scottish Qualifications Authority, in respect of HNC and HND provision;
- the Student Awards Agency Scotland (SAAS) and other statutory funding bodies;
- UK Visas and Immigration (UKVI), in respect of internationally sponsored students;
- placement providers, audition panels, casting directors, visiting practitioners, intimacy coordinators, and industry partners, where necessary for the delivery of the programme;
- Police Scotland, social work services, NHS Scotland, and other statutory partners, in respect of safeguarding, criminal investigations, and statutory duties;
- regulatory and ombudsman bodies, including the Information Commissioner's Office (ICO), the Office of the Independent Adjudicator for Higher Education (where applicable), and the Scottish Public Services Ombudsman (where applicable);
- Disclosure Scotland, in respect of PVG Scheme and disclosure checks;
- contracted processors providing services on the College's behalf, including IT, payroll, learning environment, library, and cloud-hosted services.

6.2 The College shall not transfer personal data outside the United Kingdom unless there are appropriate safeguards in place, as required by Articles 44 to 49 of the UK GDPR, including adequacy decisions, the International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another lawful transfer mechanism.

6.3 All disclosures shall be made in accordance with the data protection principles, applicable lawful bases, and the College's confidentiality obligations. The College shall not disclose personal data in response to informal requests from family members, partners, sponsors, or others without the data subject's consent, save where disclosure is necessary to protect vital interests or as required by law.

7. Information Security – Governance and Principles

7.1 The College's information security framework is designed to protect the confidentiality, integrity, and availability of information held by the College, in accordance with the UK GDPR's requirement for appropriate technical and organisational measures (Article 32) and with good practice including the Cyber Essentials framework.

7.2 The College shall apply the following information security principles:

- risk-based approach: the strength of controls shall be proportionate to the sensitivity and value of the information and the risks identified;
- least privilege: access to information and systems shall be limited to those who need it for their role;
- defence in depth: multiple layers of technical, physical, and organisational controls shall be applied;
- security by design: information security shall be considered at the design stage of new systems, processes, and partnerships, including Data Protection Impact Assessments where required;
- accountability: roles and responsibilities for information security shall be clearly defined.

8. Information Classification

8.1 All College information shall be classified in accordance with the four-tier framework set out in the Records Management and Data Retention Policy:

- Public – information that is or may be freely disclosed (for example, prospectuses, public webpages, published policies);
- Internal – information not classified as Public but suitable for general use within the College (for example, internal procedures, routine internal correspondence);
- Confidential – information that requires controlled access (for example, personal data, financial information, contractual information);
- Strictly Confidential – information requiring enhanced safeguards (for example, Special Category Data, safeguarding records, criminal records, and information whose unauthorised disclosure could cause serious harm).

8.2 Records shall be handled in accordance with their classification, including in transmission, storage, sharing, and disposal.

9. Access Controls and Authentication

9.1 Access to College systems shall be controlled through individual user accounts with secure authentication. Generic or shared accounts shall not be used for access to personal data save where strictly necessary and approved by the IT Lead. Privileged or administrative accounts shall be used only where required and shall be logged.

9.2 Passwords shall meet the College's published complexity requirements. Multi-factor authentication shall be applied where reasonably possible, including for remote access, administrative accounts, and access to systems containing significant volumes of personal data.

9.3 Access shall be granted on a least-privilege basis, reviewed periodically, and removed promptly on a change of role or on the individual ceasing to be associated with the College.

10. Devices, Endpoints, and Removable Media

10.1 College-issued devices shall be configured and managed centrally, including with endpoint encryption, antivirus and anti-malware protection, automatic updates, and remote-wipe capability where supported.

10.2 Personal devices used for College business (including staff bring-your-own-device use, and student devices used for academic work) shall be used in accordance with the Acceptable Use of IT Policy and shall not be used to store College personal data outside approved cloud-hosted services unless authorised.

10.3 Removable media (including USB drives, external hard drives, and memory cards used for rehearsal, studio, technical, or production purposes) shall be encrypted where they contain personal data and shall be tracked and disposed of securely. Unencrypted removable media shall not be used to store or transmit Confidential or Strictly Confidential information.

10.4 Lost or stolen devices shall be reported immediately to the IT Lead and the Information Governance Lead, and shall be treated as a potential personal data breach pending investigation.

11. Email and Communications

11.1 Email shall be used in accordance with the Acceptable Use of IT Policy. College personal data shall be sent only to verified recipients, with sensitive personal data sent in encrypted form or via secure file transfer where reasonably possible.

11.2 External marketing communications shall be issued in accordance with the Privacy and Electronic Communications Regulations 2003 and the UK GDPR, with appropriate consent or other lawful basis recorded.

11.3 Where staff or students use personal email accounts or messaging applications, College personal data shall not be transferred to or stored in such accounts.

12. Networks, Cloud Services, and Third-Party Suppliers

12.1 The College's networks shall be protected by appropriate firewalls, network segmentation, and intrusion monitoring. Wireless networks shall be secured with appropriate encryption and authentication.

12.2 Cloud-hosted services shall be procured only where the supplier provides appropriate contractual safeguards under Article 28 of the UK GDPR, including a data processing agreement, sub-processor controls, security commitments, breach notification commitments, and arrangements for international data transfers where applicable.

12.3 A register of contracted data processors shall be maintained by the Information Governance Lead, and contracts shall be reviewed periodically.

13. Physical Security

13.1 College premises shall be subject to appropriate physical security arrangements, including access controls to staff areas, secure storage for paper records containing personal data, controlled visitor access, and CCTV where deployed.

13.2 Paper records containing personal data shall be stored securely when not in use and shall not be left unattended in public or shared spaces. Disposal of paper records containing personal data shall be undertaken by secure shredding.

13.3 Studios, rehearsal rooms, theatres, and production areas may contain recordings, scripts, casting notes, and other personal data; these shall be handled in accordance with the classification framework and shall not be left accessible to those without authorisation.

14. Use of Images, Audio, and Video Recordings

14.1 Photographs, audio, and video recordings of identifiable individuals are personal data. The College uses such recordings for educational, formative, summative assessment, archival, promotional, and audition-feedback purposes, and may also use them for safeguarding and security purposes.

14.2 The lawful basis for use of recordings varies by purpose. Use for the educational contract relies on the contract basis; use for promotional materials, audition reels, and prospectuses requires the data subject's consent. Consent shall be recorded and may be withdrawn at any time.

14.3 Use of recordings of students under the age of 18 requires the consent of a parent or guardian and additional safeguards under the Safeguarding Policy.

15. Data Protection Impact Assessments

15.1 Where a new processing activity, system, project, or partnership is likely to result in a high risk to the rights and freedoms of individuals, the College shall undertake a Data Protection Impact Assessment (DPIA) before the processing begins, in accordance with Article 35 of the UK GDPR.

15.2 DPIAs shall be undertaken or coordinated by the Information Governance Lead and shall consider necessity, proportionality, risks, and mitigations. Where a DPIA indicates a high residual risk that cannot be mitigated, the College shall consult the Information Commissioner's Office before commencing the processing.

16. Personal Data Breaches

16.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

16.2 All actual or suspected personal data breaches shall be reported immediately to the Information Governance Lead and, where appropriate, to the IT Lead. The College shall investigate, contain, and mitigate the breach, and shall maintain a record of the breach, the investigation, and the actions taken.

16.3 Where the breach is likely to result in a risk to the rights and freedoms of individuals, the College shall notify the Information Commissioner's Office without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the breach, in accordance with Article 33 of the UK GDPR.

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

17. Training and Awareness

17.1 All staff shall undertake data protection and information security training appropriate to their role on appointment and at regular intervals thereafter, and shall be made aware of this Policy.

17.2 Staff in roles handling significant volumes of personal data, or Strictly Confidential information, shall receive enhanced training, including in relation to safeguarding, UKVI sponsorship duties, and the handling of Special Category Data.

17.3 Students shall be made aware of their responsibilities under this Policy, the Acceptable Use of IT Policy, and the Privacy Notice at Schedule 2.

18. Roles and Responsibilities

18.1 The Unibridge Group Board holds overall responsibility for the College's information governance and data protection arrangements, including approval of this Policy.

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

18.3 The Information Governance Lead is responsible for the operational implementation of this Policy, the provision of advice and guidance, the maintenance of the College's records of processing, the handling of data subject rights requests, the management of personal data breaches, and reporting to the Unibridge Group Board. The College may appoint the same officer as Data Protection Officer where appropriate.

18.4 The IT Lead is responsible for the technical implementation of information security controls, the management of IT systems and networks, the configuration of College-issued devices, and the operation of monitoring and detection arrangements.

18.5 Heads of Department, Course Leaders, and managers are responsible for the implementation of this Policy in their areas, including ensuring staff and students under their direction comply with this Policy.

18.6 All members of staff, students, and authorised third parties who handle personal data or access College systems are responsible for complying with this Policy and the Acceptable Use of IT Policy.

19. Monitoring, Review, and Enforcement

19.1 Compliance with this Policy shall be monitored through periodic review by the Information Governance Lead and reporting to the Academic Board and the Unibridge Group Board.

19.2 Breaches of this Policy by staff may be addressed under the Staff Disciplinary Procedure. Breaches by students may be addressed under the Student Code of Conduct and Disciplinary Regulations. Breaches by third parties may result in restriction or termination of access and engagement.

19.3 This Policy shall be reviewed annually, or earlier where required by legislative, regulatory, operational, or validating partner changes.

Schedule 1 – Applicant Privacy Notice

This Privacy Notice explains how GAMTA handles personal data about applicants to its programmes of study, in accordance with the UK GDPR and the Data Protection Act 2018.

S1.1 Who We Are

S1.1.1 GAMTA is the data controller for personal data about applicants. Enquiries about this Notice and about the handling of personal data should be addressed to the Information Governance Lead at the College's contact address.

S1.2 Categories of Personal Data We Collect

S1.2.1 We may collect the following categories of personal data about applicants:

- identification and contact details (full name, date of birth, address, email, telephone, immigration status where relevant);
- educational history, qualifications, and references;
- performance, audition, and portfolio materials, including audio-visual recordings of auditions, dance, singing, acting, or other performance work;
- personal statement, interview notes, and selection assessments;
- information about fee status, funding, and ability to meet financial obligations;
- information about disability, learning differences, mental and physical health, where disclosed for the purposes of reasonable adjustments (Special Category Data);
- information about criminal convictions, where disclosed under the Rehabilitation of Offenders Act 1974 and related legislation, or following PVG or Disclosure Scotland checks where required;
- immigration and right-to-study evidence, where applicable;
- equality monitoring information, where provided.

S1.3 How We Use Your Personal Data

S1.3.1 We use applicant personal data to:

- process applications, manage auditions and interviews, and reach admissions decisions;
- communicate with applicants about the application, the College, and offer arrangements;
- verify identity, qualifications, immigration status, and references;
- consider applications for funding, scholarships, and fee waivers;
- comply with statutory duties, including safeguarding, equality, immigration, and counter-terrorism duties;
- undertake equality monitoring and admissions analysis in anonymised form;
- manage applicant complaints under the Admissions Complaints Procedure.

S1.4 Lawful Basis

S1.4.1 We rely on the following lawful bases under Article 6 of the UK GDPR: steps taken at the request of the applicant prior to entering into a contract; compliance with legal obligations; performance of a task in the public interest; and our legitimate interests in considering applications and managing the admissions process. For Special Category Data, we rely on conditions under Article 9, including substantial public interest and the equality of opportunity condition under Schedule 1 to the Data Protection Act 2018.

S1.5 Sharing of Applicant Data

S1.5.1 We share applicant personal data only where necessary, including with the validating partner (in respect of validated higher education programmes); relevant Scottish awarding bodies; statutory funding bodies including SAAS; UK Visas and Immigration (for sponsored international applicants); referees; contracted processors (including IT and audition platforms); and statutory authorities where required. We do not sell applicant data.

S1.6 Retention

S1.6.1 Personal data relating to unsuccessful applicants is normally retained for one (1) year following the application cycle. Personal data relating to applicants who enrol becomes part of the student record and is retained in accordance with the Student Privacy Notice and the Records Management and Data Retention Policy.

S1.7 Applicant Rights

S1.7.1 Applicants have the rights described at Section 5 of this Policy, including the right of access, the right to rectification, and the right to object. Requests should be made to the Information Governance Lead. Applicants have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk.

Schedule 2 – Student Privacy Notice

This Privacy Notice explains how GAMTA handles personal data about its students, in accordance with the UK GDPR and the Data Protection Act 2018.

S2.1 Who We Are

S2.1.1 GAMTA is the data controller for personal data about students. Enquiries about this Notice and about the handling of personal data should be addressed to the Information Governance Lead at the College's contact address.

S2.2 Categories of Personal Data We Collect

S2.2.1 We may collect and process the following categories of personal data about students:

- identification and contact details, including next-of-kin and emergency contact information;
- educational history, qualifications, references, and academic records, including transcripts, assessment marks, examiner comments, and award classifications;
- attendance and engagement records;
- rehearsal, studio, technical, production, and performance records, including audio-visual recordings made for educational, assessment, archival, and audition reel purposes;
- casting decisions, role allocations, and intimacy and contact protocols;
- placement information and placement provider records;
- financial information, including tuition fees, SAAS records, bursary and scholarship records, and payment history;
- information about disability, learning differences, mental and physical health, including counselling records and Individual Support Plans (Special Category Data);
- safeguarding records, where applicable (handled in accordance with the Safeguarding Policy);
- disciplinary and complaints records, including academic misconduct, conduct cases, and academic appeals;
- immigration and UKVI sponsorship records (for internationally sponsored students once recruitment commences);
- information about criminal convictions and PVG Scheme membership, where relevant to the programme;
- equality monitoring information;
- CCTV recordings on College premises;
- information arising from use of College IT systems, including learning environment activity logs, email, and library use.

S2.3 How We Use Your Personal Data

S2.3.1 We use student personal data to:

- provide the programme of study, including teaching, rehearsals, studio practice, productions, performances, placements, assessment, and award conferment;
- manage the student record, registration, enrolment, attendance, and progression;
- monitor attendance and engagement, including for the purposes of UKVI sponsorship duties;
- provide student support services, including academic, financial, wellbeing, accessibility, mental health, and pastoral support;
- operate complaints, appeals, fitness to study, harassment and misconduct, and disciplinary procedures;
- collect tuition fees and other charges, and manage funding arrangements with SAAS and other funding bodies;
- comply with statutory duties, including safeguarding, equality, health and safety, immigration, and counter-terrorism duties;
- communicate with students about their studies, College services, and the College's activities;
- issue alumni communications and support graduate engagement;
- undertake quality assurance, programme monitoring, statistical analysis, and reporting, normally in anonymised form;
- use images, audio, and video recordings for educational, assessment, archival, and (with consent) promotional purposes.

S2.4 Lawful Basis

S2.4.1 We rely on the following lawful bases under Article 6 of the UK GDPR: performance of the educational contract with the student; compliance with legal obligations; performance of a task in the public interest in respect of higher and further education; the College's legitimate interests; vital interests in safeguarding and emergency situations; and consent for specific activities such as marketing communications, alumni engagement, and certain uses of images and recordings. For Special Category Data, we rely on conditions under Article 9, including health and social care, substantial public interest, and the safeguarding of children and adults at risk.

S2.5 Sharing of Student Data

S2.5.1 We share student personal data only where necessary, including with the validating partner (for validated higher education programmes); relevant Scottish awarding bodies, including the SQA; SAAS and other statutory funding bodies; UK Visas and Immigration (for internationally sponsored students); placement providers and industry partners; external examiners; Police Scotland, NHS Scotland, social work services, and other statutory partners (in safeguarding, criminal investigations, and statutory duties); regulators and ombudsman bodies (including the ICO, OIA where applicable, and the SPSO where applicable); Disclosure Scotland; contracted processors providing services on the College's behalf; and, with consent, alumni networks and casting and industry contacts.

S2.6 Retention

S2.6.1 Personal data is retained in accordance with the Records Management and Data Retention Policy and the Operational Records of Processing Schedule. Indicative retention periods include: academic transcripts and award records – permanent (summary record); student record – end of registration plus six (6) years; financial records – six (6) years plus current; safeguarding records – seventy-five (75) years from the last entry; UKVI sponsorship records –

one (1) year following the end of sponsorship, or as required by UKVI; CCTV – normally thirty-one (31) days unless retained for investigation.

S2.7 Use of Images and Recordings

S2.7.1 Recordings made of rehearsals, studio practice, and performance assessment form part of the educational programme and are made under the contract lawful basis. Use of recordings for promotional materials, prospectuses, audition reels, public-facing programme content, or for purposes beyond the educational contract requires the student's separate consent, which may be withdrawn at any time. Recordings of students under the age of 18 are subject to additional safeguards under the Safeguarding Policy.

S2.8 Student Rights

S2.8.1 Students have the rights described at Section 5 of this Policy, including the right of access, the right to rectification, the right to object, and rights in relation to automated decision-making. Requests should be made to the Information Governance Lead. Students have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk.

S2.9 Changes to This Notice

S2.9.1 This Notice may be updated from time to time. Material changes shall be communicated to students through the College's usual communication channels and the current version shall be published on the College's website.

END OF POLICY