Data Protection Policy

Protecting personal data with integrity, accountability, and trust across all areas of College life.

Document Control

Document Title	Data Protection Policy
Reference	SLP-GOV-08
Last Review	August 2024
Next Review	August 2025
Reviewer	GW
Approved by	Senior Leadership Team
Version	2.0

Contents

1. About This Policy

Our Commitment

At SLP College, the privacy and integrity of every individual's personal data is fundamental to our values and operations. This policy clearly sets out how we fulfil our responsibilities under UK data protection legislation, how we use and safeguard personal data, and how individuals can exercise their data protection rights.

By implementing this policy effectively, we ensure that we:

- Meet or exceed our legal obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant provisions of the Privacy and Electronic Communications Regulations (PECR).
- Operate transparently and fairly, building trust across the SLP community, including students, staff, alumni, and external stakeholders.
- Maintain robust accountability frameworks and practices, embedding data protection into our daily working culture.

Who This Policy Applies To

This policy covers all personal data processed by, or on behalf of, SLP College. It applies to every type of data held, digital, physical (paper-based), photographic, audio-visual, or in any other recorded format.

Specifically, it applies to all:

- Current and prospective students (including applicants who do not enrol).
- Alumni and former students.
- Staff members (including permanent, fixed-term, part-time, freelance, visiting professionals, volunteers, and trustees).
- Contractors, consultants, suppliers, partners, and service providers.
- Audience members, visitors, guests, or any other third parties whose personal data SLP College processes.

Compliance and Enforcement

This policy is mandatory for all SLP College staff, associates, and third-party contractors who handle or process personal data as part of their role. Non-compliance may lead to disciplinary action, contractual sanctions, or, in serious cases, legal action.

If you have questions or uncertainties regarding your obligations under this policy or data protection law, you must contact the Data Protection Officer (DPO) immediately for guidance before proceeding.

Ignorance or misunderstanding of these obligations will not be accepted as an excuse for non-compliance.

Policy Ownership and Governance

SLP College's Senior Leadership Team (SLT) is responsible for this policy as the Data Controller, overseeing all institutional data protection activities.

The policy is formally reviewed at least once per academic year by the Data Protection Officer in collaboration with the SLT. Reviews will also occur promptly whenever there are relevant legislative changes, significant shifts in regulatory guidance, internal operational changes, or in response to any identified data protection incidents or audits.

Each review ensures our ongoing legal compliance, operational relevance, and continued alignment with the College's mission, vision, and values.

2. Key Definitions

To help everyone at SLP College clearly understand their responsibilities, the following terms are defined according to UK data protection law. If you encounter these terms within the policy, refer back to this section for clarity.

Personal Data

Information relating to a living person who can be identified, either directly from the data itself or indirectly from the data combined with other available information.

Examples at SLP College include:

- Names and addresses.
- Email addresses and contact numbers.
- Student and staff ID numbers.
- Images (photos or videos), voice recordings.
- Online identifiers, such as IP addresses or usernames.

Special Category Data.

Highly sensitive personal data requiring special handling and protections due to its confidential nature.

This includes data revealing:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.

- Genetic data and biometric identifiers (e.g. fingerprint scans).
- Health information (mental or physical).
- Sex life or sexual orientation.

SLP College may only process this type of data under specific lawful conditions.

Criminal Offence Data

Information relating to criminal convictions, alleged criminal activity, or related legal proceedings.

This data is strictly controlled and can only be processed in accordance with UK law and under defined conditions.

Data Subject

An individual whose personal data is collected, held, or processed by SLP College.

Typical data subjects include:

- Students, including applicants and alumni.
- Staff members and freelance professionals.
- Visitors, contractors, suppliers, and guests.

Processing

Any operation involving personal data, either automated or manual.

This broadly includes:

- Collecting and recording.
- Organising or storing.
- Adapting or altering.
- Retrieving or consulting.
- Sharing, disclosing, or transmitting.
- Restricting or deleting.

If you handle personal data as part of your role at SLP College, you are processing it.

Data Controller

The organisation or individual legally responsible for deciding how and why personal data is processed.

SLP College is the Data Controller for all personal data associated with its educational and administrative activities.

Data Processor

An external individual or organisation that processes personal data strictly on behalf of the Data Controller (SLP College), under contractual obligations.

Examples include:

- Payroll providers.
- External IT service providers managing student records systems.

Data Protection Officer (DPO)

A designated role within SLP College is to oversee compliance with data protection laws.

The DPO's responsibilities include:

- Advising staff and management on their data protection obligations.
- Monitoring internal compliance and conducting regular audits.
- Providing training and awareness for staff.
- Handling data protection queries, subject access requests, complaints, and breaches.
- Liaising directly with the Information Commissioner's Office (ICO).

All staff should consult the DPO when unsure about data protection procedures or responsibilities.

The Data Protection Officer for SLP College is: Gary Wood, Head of Operations

Consent

Freely given, specific, informed, and unambiguous agreement provided by a data subject for their personal data to be processed.

Valid consent must be:

- Clearly and actively given by the data subject (e.g. ticking a box, signing a consent form).
- Documented and easy to withdraw at any time.
- Specific to the data collected and its intended use.

At SLP College, consent is never assumed or inferred from silence or inactivity.

Subject Access Request (SAR)

A formal request by a data subject to see copies of their own personal data held by SLP College.

When a SAR is received, the College must respond promptly, within one calendar month.

Personal Data Breach

A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples include:

- Accidental emailing of confidential data to the wrong recipient.
- Lost or stolen laptop or storage device containing unencrypted personal data.
- Cyberattack resulting in compromised student or staff records.

Any suspected breach, however minor, must be reported immediately to the DPO.

Pseudonymisation

The processing of personal data in a manner that prevents identification without additional information.

For example, ID numbers or codes instead of names should be used, provided that the additional identifying information is stored separately and securely.

Anonymisation

Irreversibly removing or obscuring personal identifiers from data so individuals can no longer be identified, directly or indirectly.

Once data is fully anonymised, it is no longer classified as personal data under the law.

Third Party

Any external individual or organisation other than the data subject, the Data Controller (SLP College), or authorised Data Processors.

Information Commissioner's Office (ICO)

The UK's independent regulatory body is responsible for overseeing compliance with data protection legislation, including the UK GDPR and the Data Protection Act 2018.

3. Legal and Regulatory Framework

SLP College is committed to complying with all applicable laws and regulatory requirements governing the handling of personal data. This section outlines the core legislative and regulatory foundations that underpin our data protection responsibilities and guide our operations. Every individual associated with SLP College must understand and consistently adhere to these requirements.

UK General Data Protection Regulation (UK GDPR)

The UK GDPR is the cornerstone of UK data protection legislation, providing comprehensive rules for handling personal data. Effective since 1 January 2021, the UK GDPR mirrors the EU GDPR, establishing a robust framework for data protection compliance.

Key provisions include:

- Clear principles for lawful, fair, and transparent data processing.
- Defined rights for data subjects (individuals whose data we handle).
- Specific legal grounds are required for processing personal data.
- Obligations to protect data and demonstrate accountability.
- Mandatory reporting of certain data breaches.

Compliance with UK GDPR is not optional; failure to comply can result in substantial penalties, regulatory action, and reputational harm.

Data Protection Act 2018 (DPA 2018)

The DPA 2018 complements and extends the UK GDPR, providing specific conditions under which personal data, particularly special category and criminal offence data, can lawfully be processed.

The DPA 2018:

- Establishes conditions for processing sensitive data categories.
- Details certain exemptions (e.g., for safeguarding, crime prevention, and legal proceedings).
- Defines criminal offences relating to the unlawful handling or disclosure of personal data.
- Grants enforcement powers to the Information Commissioner's Office (ICO).

Understanding and complying with the DPA 2018 ensures SLP College handles sensitive data securely and lawfully.

Privacy and Electronic Communications Regulations (PECR)

PECR governs electronic communications, including email marketing, the use of cookies, and digital communications privacy.

SLP College must adhere to PECR requirements when:

- Conducting direct marketing activities (Email or SMS).
- Operating websites and digital platforms using cookies.
- Managing electronic communications systems (e.g., student or parent email lists, marketing newsletters).

- The ICO monitors PECR compliance and is complementary to UK GDPR requirements.

Sector-Specific and Supplementary Requirements

SLP College is subject to additional statutory and regulatory standards directly relevant to our educational, safeguarding, and operational activities. These requirements include, but are not limited to:

- **Office for Students (OfS) Conditions of Registration:** Mandate effective governance arrangements for personal data, aligned with transparency and accountability standards essential for regulatory compliance and registration.
- **Ofsted Inspection Framework:** Requires robust data management practices, especially relating to safeguarding, learner records, and inspection readiness, to demonstrate educational effectiveness and statutory compliance.
- **UK Visas and Immigration (UKVI):** Establishes data processing requirements for international students and visa sponsorship records, requiring stringent compliance to maintain sponsorship status.
- **Protection of Freedoms Act 2012:** It regulates biometric data processing (such as fingerprinting and facial recognition), which is particularly relevant to learners aged under 18, requiring explicit consent and clearly documented safeguards.
- **Safeguarding and Child Protection Legislation (e.g., KCSIE):** Requires secure, lawful, and proportionate information sharing with safeguarding authorities to protect students' welfare effectively.
- **Freedom of Information Act 2000 (FOIA):** Sets standards for responding to information requests from the public sector, impacting how data may be disclosed or protected.

Guidance and Regulatory Oversight

In fulfilling our legal responsibilities, SLP College actively refers to guidance and codes of practice provided by regulatory authorities and sector bodies, notably:

- **The Information Commissioner's Office (ICO):** Guide to the UK GDPR, Data Sharing Code of Practice, Guidance on Subject Access Requests.
- **The Department for Education (DfE):** Data Protection Toolkit for Schools and Colleges, Keeping Children Safe in Education (KCSIE), guidance on safeguarding data management.
- **Advance HE and Conservatoires UK (CUK):** Best-practice guidance and sector benchmarking for data governance and accountability in conservatoire and HE settings.

Institutional Responsibilities and Accountability

As the Data Controller, SLP College is legally and ethically accountable for ensuring all personal data is processed strictly in accordance with the frameworks outlined in this section.

SLP College ensures compliance through:

- Clearly defined policies, procedures, and responsibilities.
- Staff training and regular refresher updates.
- Internal audits and compliance monitoring.
- Transparent breach-reporting and remediation processes.

SLP College also ensures that external data processors acting on our behalf are bound by written agreements requiring equivalent standards of data protection.

Consequences of Non-Compliance

Failure to comply with any aspect of the laws and regulations described above may result in:

- Enforcement action by regulatory bodies (ICO, OfS, Ofsted).
- Substantial financial penalties or legal sanctions.
- Damage to the College's reputation and public trust.

All staff, contractors, associates, and third parties must uphold SLP College's data protection standards at all times. Ignorance is not a defence. If you have questions or require clarification, seek advice promptly from the Data Protection Officer.

This comprehensive, structured framework underpins our robust approach to personal data management, safeguarding the trust of our stakeholders and supporting the College's mission, vision, and values.

4. Our Commitment to Data Protection

At SLP College, protecting personal data is central to our professional integrity, educational mission, and institutional reputation. Our approach to data protection exceeds basic compliance, reflecting our fundamental commitment to trust, accountability, and transparency in all our relationships.

This section clearly defines the principles that guide our collection, use, storage, and management of personal data, ensuring every staff member, student, and stakeholder understands our standards and responsibilities under UK law.

Core Data Protection Principles

SLP College rigorously adheres to the six data protection principles enshrined in the UK General Data Protection Regulation (UK GDPR). Every individual processing personal data at the College must consistently apply these principles:

Principle	What This Means for SLP College
1. Lawfulness, Fairness, and Transparency	We always process personal data lawfully, ethically, and openly, clearly communicating what we do, why we do it, and how we safeguard data.
2. Purpose Limitation	We clearly define our reasons for processing personal data, and never use that data for unrelated purposes.
3. Data Minimisation	We collect only the personal data we genuinely need to meet a clearly defined purpose and never more than necessary.
4. Accuracy	We proactively keep personal data accurate and current, promptly correct errors and respond quickly to requests to update information.
5. Storage Limitation	We keep personal data no longer than needed to fulfil the purpose for which it was collected, securely deleting or anonymising it as soon as possible thereafter.
6. Integrity and Confidentiality	We maintain robust technological and organisational security measures to protect personal data against loss, unauthorised access, or misuse.

These principles are fundamental, non-negotiable standards that all staff, contractors, visiting professionals, and volunteers at SLP College are required to uphold without exception.

Accountability: Demonstrating Our Compliance

SLP College recognises that simply meeting data protection obligations is insufficient; we must also be able to demonstrate compliance. This requirement, known as the accountability principle, means that we proactively manage data protection through clear structures, documentation, and transparent governance.

To ensure accountability, SLP College:

- Maintains accurate and detailed records of data processing activities, including lawful bases and data retention periods.
- Publishes clear, regularly updated privacy notices and policies to inform data subjects precisely how their personal data is used.
- Implements Data Protection Impact Assessments (DPIAs) proactively whenever new projects, systems, or significant data processing changes are considered.
- Regularly reviews and audits data protection practices internally, quickly rectifying any identified compliance gaps or risks.
- Provides regular data protection training, awareness initiatives, and continuous guidance tailored to staff roles and responsibilities.
- Has clearly defined reporting procedures to promptly address and rectify any personal data breaches, concerns, or queries.

Accountability is built into every level of our College structure, from strategic decision-making by the Senior Management Team to the daily operations of every department.

Embedding a Strong Data Protection Culture

SLP College is committed to embedding data protection into all aspects of institutional life. This includes:

- **Strong Leadership:** The Senior Leadership Team (SLT) actively promotes a culture of data protection, ensuring that legal and ethical obligations are considered at every strategic decision point.
- **Privacy by Design:** Data protection considerations are integrated from the very beginning into any new project, service, or system implementation, not as an afterthought.
- **Consistent Training and Awareness:** All staff receive induction training on data protection, as well as regular updates and refresher training to ensure continuing competence and awareness.
- **Clear Governance Structures:** Responsibility for data protection is explicitly assigned within each team or department and overseen by the Data Protection Officer, ensuring effective local accountability.
- **Transparency with Stakeholders:** Clear and accessible privacy notices inform our students, staff, alumni, and third parties precisely how we manage their personal data, enhancing trust through clarity.

Staff and Associate Responsibilities

All staff, contractors, freelancers, and volunteers at SLP College have clear responsibilities under this policy. Each individual is expected to:

- Understand and apply the six data protection principles in their everyday activities.
- Access and process only the personal data strictly necessary for their role.
- Keep personal data secure, confidential, and accurate at all times.
- Immediately report data breaches, errors, or compliance concerns to the Data Protection Officer.
- Participate fully in data protection training, ensuring personal compliance and institutional readiness for audits or inspections.

Failure to adhere to these standards may lead to disciplinary action, contractual sanctions, or legal consequences, reflecting the seriousness of our institutional commitment to data protection.

Trust, Transparency, and Continuous Improvement

At SLP College, data protection goes beyond compliance; it is integral to our relationship with every individual we engage with. We commit to a culture of continuous improvement, regularly reviewing and updating our practices to ensure:

- **Trust:** Individuals have confidence in how we manage and protect their personal data.

- **Transparency:** Our data handling processes are clear, fair, accessible, and openly communicated.
- **Integrity:** Every interaction we have involving personal data upholds the highest ethical standards and institutional values.

Our unwavering commitment to these principles and practices ensures we handle all personal data responsibly, professionally, and in full compliance with the law, sustaining trust at every level of our community.

5. Roles and Responsibilities

Effective data protection at SLP College requires clear accountability, structured governance, and a shared understanding of individual and collective responsibilities. Every person who engages with personal data at SLP College must clearly understand their role and obligations and adhere strictly to our high standards.

This section precisely defines responsibilities at every level of the College, ensuring legal compliance, operational clarity, and institutional integrity under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

SLP College as Data Controller

SLP College is the Data Controller for all personal data it processes as part of its operational, educational, and administrative activities. As a Data Controller, the College has ultimate legal responsibility for:

- Determining what personal data is collected, why it is collected, and how it is processed.
- Ensuring all personal data processing is lawful, transparent, fair, and secure.
- Maintaining robust documentation and evidence of compliance with data protection laws.

The Senior Leadership Team (SLT) holds collective institutional accountability, ensuring that:

- Data protection is embedded into strategic decisions and operational practices.
- Sufficient resources, training, and support are provided to ensure compliance.
- Clear policies, frameworks, and governance structures are established and maintained.

A culture of proactive data protection awareness and compliance is consistently promoted.

Data Protection Officer (DPO)

SLP College appoints a Data Protection Officer (DPO), who operates independently and objectively to oversee and guide the College's data protection compliance.

The DPO's core responsibilities include:

- Advising SLT, managers, staff, and contractors on their data protection obligations under UK GDPR and related laws.
- Monitoring compliance with this policy, conducting audits, and recommending improvements.
- Coordinating and providing regular training, guidance, and awareness-raising for staff.
- Managing the College's response to Subject Access Requests (SARs), personal data breaches, and ICO communications.
- Reviewing and advising on Data Protection Impact Assessments (DPIAs) for high-risk activities and projects.
- Acting as the central point of contact for data protection queries, concerns, or incidents internally and externally.

The DPO reports directly to SMT, maintains institutional independence, and must be consulted promptly in relation to any significant data protection matters.

The DPO for SLP College is: Gary Wood, Head of Operations.

Senior Leadership Team (SLT) and Senior Leaders

The SLT and senior leaders within SLP College have explicit responsibilities for embedding data protection throughout the College, including:

- Ensuring that departmental practices and projects comply fully with data protection requirements.
- Consulting and collaborating proactively with the DPO on all data protection issues or risks.
- Modelling and promoting best-practice standards and institutional policies in all decisions and actions.
- Ensuring adequate staff training, support, and clear guidance on data protection obligations.
- Regularly review departmental compliance and take prompt action when gaps or risks are identified.

Heads of Department and Managers

Heads of Departments and Managers must take personal and departmental responsibility for data protection compliance, including:

- Implementing and enforcing this policy consistently within their teams.
- Supporting staff to understand and comply with their responsibilities.
- Maintaining accurate and timely records of personal data activities in their area (where required).

- Immediately reporting any data protection incidents, concerns, or potential breaches to the DPO.
- Engaging proactively with the DPO when considering new projects, systems, or significant data processing changes.

All Staff, Visiting Professionals, Freelancers, and Volunteers

Every staff member and associate at SLP College shares a personal and professional responsibility for protecting personal data. Individuals must:

- Familiarise themselves with this policy, attend required training, and comply with data protection standards.
- Handle personal data strictly within the bounds of their role and authorised purposes.
- Maintain data confidentiality and security at all times, using College-approved systems and protocols only.
- Ensure personal data is accurate, complete, and updated promptly where necessary.
- Immediately report any concerns, errors, or breaches to their manager or directly to the DPO.

Non-compliance with these standards may result in disciplinary, contractual, or legal consequences.

Data Processors and External Suppliers

SLP College engages external organisations (known as Data Processors) only where strict written contracts and controls are in place. Data Processors are responsible for:

- Processing personal data only according to explicit, documented instructions provided by SLP College.
- Implementing robust technical and organisational measures to safeguard personal data at a level equal to or exceeding that required by UK GDPR.
- Immediately notifying SLP College of any personal data breach, security incident, or data subject request they receive.
- Assisting SLP College in meeting compliance obligations, including audit support and cooperation with data subject requests or ICO queries.

Any external partner or supplier found to process data outside contractual boundaries or without appropriate safeguards will be subject to immediate review and potential termination of services.

Responsibilities of Data Subjects (Students, Applicants, Staff, Alumni, Others)

Individuals whose data SLP College processes also have responsibilities to help maintain the integrity of their data, including:

- Ensuring that any personal data provided to the College is accurate, complete, and updated promptly if it changes.
- Reading and understanding relevant privacy notices, and asking questions if uncertain about data usage.
- Exercising their data protection rights (e.g. subject access, correction) in line with College processes clearly outlined in privacy communications.

Reporting, Oversight, and Escalation

Clear reporting and escalation pathways exist for all data protection issues:

- Any concern or suspected breach must be reported immediately to the Data Protection Officer.
- Managers must escalate significant risks or compliance issues to the SLT without delay.
- The DPO maintains clear records of incidents, breaches, and compliance measures, regularly reporting to SLT and external regulators (ICO, OfS, Ofsted) as required.

Delayed or non-reporting of data protection issues may significantly increase risk, harm individuals' rights, and expose the College to regulatory action. Therefore, immediate and transparent reporting is mandatory.

6. What Personal Data We Collect and Our Legal Basis for Processing

At SLP College, we collect personal data only when necessary, justified, and lawful. This section transparently details the types of personal data we handle, the individuals to whom the data relates, and the legal justifications we rely upon to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

We always limit the personal data we collect to the minimum required to achieve our operational, educational, or legal responsibilities.

Types of Personal Data We Collect

Depending on the relationship between an individual and the College, we may process the following categories of personal data:

Data Subjects	**Categories of Personal Data Processed**
Students & Applicants	Name, date of birth, contact details, audition records, academic assessments, attendance, ID documents, images/videos for performance or promotional purposes, financial information for fees and bursaries, emergency contacts, safeguarding disclosures, and medical/health conditions.
Staff & Visiting Professionals	Name, contact information, employment and educational history, DBS checks, payroll/tax information, right-to-work documentation, absence and

	appraisal records, performance evaluations, training and professional development records, photographs or audio-visual recordings, safeguarding information (where applicable).
Alumni	Name, contact information, graduation history, employment information (where provided), event attendance, and alumni engagement preferences.
Contractors & Suppliers	Contact details, contract terms, professional accreditations, compliance records, and financial/payment information.
Audience & Visitors	Ticketing information, event registrations, contact details (when provided), marketing preferences, feedback or queries submitted via digital channels.

Special Category and Criminal Offence Data

SLP College occasionally processes sensitive personal information known as special category data, including:

- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Physical or mental health conditions.
- Sexual orientation or gender identity.
- Disability status or specific access needs.
- Biometric identifiers (e.g., photographs or identification methods).
- Political opinions (only if voluntarily disclosed).

We also process criminal offence data, primarily through:

- Disclosure and Barring Service (DBS) checks for staff and certain contractors.
- Records relating to safeguarding incidents or allegations.

Such data is processed strictly under conditions set by the Data Protection Act 2018 and UK GDPR, with additional robust security measures and confidentiality requirements applied.

Legal Basis for Processing Personal Data

To comply with UK GDPR Article 6, we rely on the following lawful bases for processing personal data:

Legal Basis	**How We Apply It at SLP College**
Contractual Obligation	Processing necessary to fulfil educational agreements (e.g., enrolment, course delivery, assessments) or employment contracts (staff salary and HR functions).
Legal Obligation	Data processing required by law (e.g., UKVI immigration compliance, HMRC payroll reporting, safeguarding duties, statutory audits).
Legitimate Interests	Used for operational needs balanced against individual rights (e.g., alumni communications, internal quality assurance processes, general administrative activities, audience/event management).
Vital Interests	Processing to protect life or safety (e.g., emergency medical care, urgent safeguarding interventions).

Public Task	Data processing is in the public interest, particularly related to providing education and supporting educational regulations and standards.
Consent	Explicit consent is obtained where necessary (e.g., promotional marketing, photography, optional surveys, or voluntary disclosures). Consent is always specific, freely given, informed, and withdrawable at any time.

Consent is never the default legal basis for processing at SLP College; it is utilised selectively, transparently, and only when other legal bases do not apply or where an explicit choice is required.

Legal Conditions for Processing Special Category and Criminal Offence Data

Special category and criminal offence data require explicit conditions under Article 9 of UK GDPR or Schedule 1 of the DPA 2018, including:

- Explicit consent (e.g., health or disability information to provide student support services).
- Employment and social protection law (staff occupational health, absence management).
- Vital interests (medical emergencies, immediate safeguarding concerns).
- Substantial public interest (safeguarding, equality monitoring, preventing or detecting unlawful acts).
- Legal claims (handling disciplinary procedures, grievances, or misconduct allegations).
- Health and social care provision (student counselling or pastoral care).

For criminal offence data, processing is strictly limited to:

- DBS checks as legally required.
- Specific safeguarding activities under clear statutory authority.
- Other legal obligations as expressly permitted by law.

Our Commitment to Data Minimisation and Purpose Limitation

At SLP College, we adopt strict principles to ensure the responsible handling of personal data:

- **Data Minimisation:** We collect only the minimal personal data required to fulfil our stated purposes. We never request or store unnecessary or irrelevant information.
- **Purpose Limitation:** We clearly specify why data is collected and never repurpose it without reassessing legality and proportionality. Data is not reused for incompatible reasons without securing a new lawful basis and clearly notifying affected individuals.

Accuracy and Data Updates

We ensure personal data accuracy through proactive reviews and provide clear mechanisms for data subjects to update their information. Students and staff should promptly notify the College if their personal information changes, such as contact details, emergency contacts, or health information.

Transparency and Documentation

SLP College maintains detailed internal records of data processing activities, including lawful bases, retention periods, and data-sharing agreements. These records support transparency and demonstrate our commitment to compliance.

We communicate our processing practices clearly to individuals through detailed, accessible privacy notices provided at the point of data collection (e.g., enrolment, employment onboarding, event registration) and made publicly available on our website.

7. Rights of Individuals and How to Exercise Them

SLP College recognises that the personal data we process belongs to the individuals who entrust us with their information. Upholding data protection rights is central to our institutional commitment to respect, transparency, and accountability.

Under the UK General Data Protection Regulation (UK GDPR), individuals have clear and enforceable rights concerning their personal data. This section outlines these rights, how individuals can exercise them, and our commitment to responding promptly, transparently, and respectfully.

Your Data Protection Rights Explained

Your Right	What It Means for You
Right to be informed.	You have the right to clear and transparent information about how we collect, use, share, and protect your data. Our privacy notices provide these details clearly and specifically.
Right of Access (Subject Access Request)	You can request a copy of all personal data we hold about you, plus information on how and why we process it. This helps you verify the lawfulness of our data processing.
Right to Rectification	You can ask us to correct or update your data promptly if it's incorrect, incomplete, or outdated.
Right to Erasure (right to be forgotten)	You can request deletion of your personal data under specific circumstances, for example, if we no longer need the data or if you withdraw previously given consent.
Right to Restrict Processing	You can request that we temporarily stop processing your personal data in certain situations, such as disputes over accuracy or legality, without deleting it entirely.
Right to Data Portability	Where processing relies on your consent or contract, you can request your data in a commonly used, electronic format to transfer elsewhere easily and securely.
Right to Object	You can object to data processing based on our legitimate interests, including direct marketing or profiling. We must stop processing unless we demonstrate compelling reasons otherwise.
Rights Related to Automated Decision-Making and Profiling	You have the right not to be subject to decisions based solely on automated processing (including profiling) that significantly affect you, unless specific safeguards are in place.

How to Exercise Your Rights

To exercise any of the rights listed above, please get in touch with our Data Protection Officer (DPO) directly:

Name: Gary Wood
Email: gwood@slpcollege.co.uk
Postal Address: Data Protection Officer, SLP College, 5 Chapel Lane, Garforth, LS25 1AG

We ask you to clearly state which right you are exercising and provide relevant details to help us respond promptly and effectively. For security, we may verify your identity, especially if the request involves sensitive or special category data.

Our Commitment to Timely Responses

We respond to all valid requests promptly and within one calendar month of receipt. If your request is particularly complex or you make multiple requests, we may extend this timeline by up to two additional months, but we will inform you clearly within the first month and explain our reasons.

All responses are provided free of charge. However, if a request is clearly unfounded, excessive, repetitive, or manifestly unreasonable, we reserve the right to charge a reasonable fee or refuse the request. If refused, we will explain clearly why and inform you of your right to appeal to the ICO.

Subject Access Requests (SARs)

You have the right to obtain a clear and transparent copy of the personal data we hold about you. Specifically, you can request:

- Confirmation that your personal data is being processed.
- Access to a complete copy of your personal data.
- Details about the purposes of processing.
- Categories of personal data we process.
- Information on recipients or categories of recipients we share data with.
- The expected retention period for your data.
- The source of the data (if not obtained directly from you).
- Information on your data protection rights.
- The right to complain to the ICO.

We may withhold or partially redact data if disclosure would infringe the rights of another individual or if a clear legal exemption applies (e.g. safeguarding).

How to Withdraw Consent

If processing is based on your explicit consent, you may withdraw that consent at any time, easily and without consequence. To withdraw consent:

- Contact the DPO directly or use the provided opt-out methods in our communications.
- Withdrawal of consent will not affect the lawfulness of any processing conducted before withdrawal.
- We will immediately cease processing activities based on withdrawn consent unless another lawful basis for processing applies (and you will be informed clearly if this is the case).

Raising Concerns and Complaints

We take any concerns about personal data handling seriously and aim to resolve them quickly and transparently. If you believe your data protection rights have been compromised or mishandled, you may:

- First, raise your concern directly with our Data Protection Officer (DPO).
- Alternatively, or if not satisfied with our response, contact the Information Commissioner's Office (ICO):
  Website: ico.org.uk
  Telephone: 0303 123 1113
  Postal: ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

We encourage direct contact with us first to allow rapid resolution of concerns.

Limitations and Exceptions

Please note that certain rights under UK GDPR are not absolute and may be subject to specific legal limitations or exceptions, such as when data processing is:

- Required to comply with a legal obligation (e.g. safeguarding duties, statutory reporting, immigration laws).
- Necessary for the establishment, exercise, or defence of legal claims.
- Necessary for public interest purposes (e.g. public health emergencies).

Where such exemptions apply, we will clearly explain this in our response, including your right to challenge or escalate the decision.

Our Institutional Commitment

At SLP College, respect for individual rights over personal data is integral to our ethos. We commit fully to transparent communication, responsible data governance, and prompt, respectful handling of every rights request.

All staff and associates are trained to recognise and support your data rights effectively and respectfully. We maintain robust internal procedures, records, and safeguards to ensure your rights are consistently upheld.

8. Accessing and Sharing Personal Data

SLP College is trusted to handle personal data professionally, lawfully, and securely. This section sets out how we control internal access to personal data, under what circumstances it may be shared externally, and the safeguards we apply to every form of data disclosure.

We apply a strict "need-to-know" standard and ensure that data is only shared when there is a lawful basis, a clear purpose, and adequate protection in place. The principles of data minimisation, accountability, and security govern all access and sharing activity.

Internal Access: Role-Based, Purpose-Driven

Access to personal data within SLP College is restricted to those who need it to perform their professional duties. This means:

- No individual may access personal data outside the scope of their role, even if they have system access.
- Access rights are determined by job function and are reviewed periodically.
- Temporary or exceptional access (e.g., for audits and investigations) must be approved by a line manager and the DPO.

For example:

- A personal tutor may access their students' academic and support information but not other learners' data.
- A finance officer may access payment data but not safeguard records.

Unlawful access, including curiosity-driven browsing, is a breach of College policy and may result in disciplinary or legal action.

External Sharing: When and Why We Share Data

We only share personal data outside the College where at least one of the following applies:

- The individual has given informed consent.
- The sharing is necessary to fulfil a contract (e.g. SLC or external awarding body).
- We are legally required to share it (e.g. under UKVI, HMRC, OfS, or safeguarding legislation).
- The sharing is necessary to protect someone's life or safety (vital interests).

- The sharing is necessary to perform a task in the public interest or exercise official authority.
- We or the recipient have a legitimate interest that does not override the individual's rights.

Each data-sharing decision must be:

- **Justified:** with a clear legal basis and purpose.
- **Proportionate:** only the minimum data necessary is shared.
- **Documented:** using a data-sharing log, agreement, or DPIA if high-risk.

Common Types of External Sharing

SLP College may share data with:

Category	Purpose of Sharing
Service providers	IT systems, digital platforms, cloud storage, student record databases, payroll, HR tools.
Regulators and statutory bodies	OfS, Ofsted, UKVI, SLC, HESA, HMRC, local authorities, DfE.
Awarding or validating institutions	Where students are on externally validated courses.
Safeguarding authorities	Local authority safeguarding boards, police, and emergency services.
Professional advisers	Legal, audit, HR or compliance consultants under contract.
Parents or guardians (18+ learners)	Only with documented consent or where a serious risk to welfare is identified.
Alumni platforms and networks	With opt-in consent for communications and engagement.

All third-party recipients must provide suitable assurances that they will process the data securely, lawfully, and in line with SLP College's instructions.

Contracts with Data Processors

Where SLP College outsources processing to an external party (a Data Processor), we ensure:

- A UK GDPR-compliant contract is in place.
- The processor acts only on our documented instructions.
- The processor has appropriate security measures and a clear breach response protocol.
- The processor does not use sub-processors without College approval.
- Data is returned or securely destroyed at the end of the contract.

Examples include outsourced IT support, cloud-based systems, or assessment platforms.

No data may be shared with a processor until the DPO has reviewed and confirmed contractual adequacy.

Safeguarding and Emergency Disclosures

We may share personal data without consent where necessary to:

- Protect a child or vulnerable adult from serious harm.
- Prevent a crime or respond to law enforcement requests.
- Provide urgent medical assistance where the individual is unable to consent.

Such disclosures must be:

- Approved by the Designated Safeguarding Lead or DPO unless delay increases the risk.
- Recorded in full, including legal basis, rationale, and recipient details.
- Shared securely and limited to what is strictly necessary.

We never promise absolute confidentiality where safeguarding concerns are disclosed.

International Data Transfers

We only transfer personal data outside the UK when:

- The destination country has been assessed as offering adequate protection.
- Standard Contractual Clauses (SCCs) or International Data Transfer Agreements (IDTAs) are in place.
- Additional safeguards (e.g. encryption, limited access) are applied.
- A clear, documented legal basis supports the transfer (e.g. contract fulfilment, consent, legal obligation).

International data sharing is rare and requires DPO approval and risk assessment in all cases.

Secure Sharing Methods

All personal data must be shared using approved, secure channels. This includes:

- Encrypted Email or password-protected attachments.
- College-authorised file transfer platforms (e.g. secure cloud services).
- Role-based system access with audit logging.
- Paper documents sent by tracked or secure delivery methods, marked Private & Confidential.

Staff must never:

- Use personal Email, messaging apps (e.g. WhatsApp), or unapproved devices to transmit College data.
- Leave personal data unattended or accessible in shared spaces.

- Share passwords or delegate access without authorisation.

Any doubts about sharing methods must be referred to the DPO.

What to Do if Data is Shared Inappropriately

If data is shared by mistake (e.g. emailed to the wrong person, excessive information disclosed), you must:

- Immediately inform the DPO.
- Secure the data where possible (e.g., attempt recall or notify the unintended recipient).
- Cooperate fully with the breach response process.

Delays in reporting can increase harm and may breach the UK GDPR's 72-hour reporting window for notifiable breaches.

Logging, Oversight, and Review

The DPO maintains a Data Sharing Register that records:

- Significant or high-risk data-sharing activities.
- The legal basis for sharing.
- Any third-party arrangements or contracts in place.
- Data minimisation measures and security arrangements.

Staff involved in regular or large-scale sharing must work with the DPO to ensure compliance and audit readiness.

SLP College will never share personal data unless it is necessary, lawful, and secure. We empower staff with clear protocols and training, and we protect individuals through rigorous oversight, transparency, and legal integrity.

9. Securing Personal Data

SLP College has a professional, legal, and ethical duty to protect the personal data entrusted to us. We are committed to maintaining high standards of data security, technically, physically, and behaviourally, across every part of College life.

Data security is not just about systems. It is about discipline, vigilance, and trust.

This section sets out the College's approach to safeguarding personal data from unauthorised access, loss, damage, or misuse, whether stored digitally, on paper, or transmitted verbally.

Our Security Principles

We apply security controls based on the following principles:

- **Confidentiality:** Only authorised individuals can access personal data.
- **Integrity:** Data is accurate, reliable, and protected from unauthorised modification.
- **Availability:** Data is accessible only when needed by authorised users, through secure means.
- **Resilience:** Systems are protected against failure and designed to recover swiftly if breached or disrupted.

These principles apply to all formats, emails, databases, audio-visual materials, printed files, verbal disclosures, and cloud-based records.

Technical and Organisational Controls

SLP College applies layered safeguards that reflect the sensitivity of the data processed:

Control Area	**Examples of Measures in Place**
Access control	Role-based permissions, strong passwords, account audit logs, and least-privilege access.
Device security	Encryption, password enforcement, remote lock/wipe capability, endpoint monitoring.
System and network	Firewalls, anti-malware tools, secure Wi-Fi, multi-factor authentication (MFA), and intrusion detection.
Data storage	Use of approved cloud platforms (e.g. SharePoint, OneDrive), encrypted drives, and secure backup systems.
Email security	Encrypted Email, auto-logout, internal alerting for risky behaviour (e.g. external forwarding)
Physical security	Locked storage, access-controlled rooms, CCTV (where installed), secure destruction bins.
Monitoring and testing	Periodic audits, simulated phishing, system health checks, and vulnerability scans.

All systems and providers used for processing personal data are subject to due diligence, procurement review, and DPO oversight.

Staff and Associate Responsibilities

Every staff member, freelancer, contractor, and visiting professional is responsible for keeping personal data secure.

This means:

- Only accessing data you are authorised to use.
- Using College-approved systems, devices, and storage locations.
- Do not duplicate or export data to personal accounts or devices.
- Logging out when systems are unattended.

- Securing physical materials (e.g. assessments, health disclosures) at all times.
- Challenging poor practice and reporting risks promptly.

Security failures, whether accidental or deliberate, will be treated seriously and may lead to disciplinary or contractual action.

Remote Working and Offsite Access

When working from home, on tour, or offsite, you must maintain the same security standards as on campus.

This includes:

- Using only College-issued or authorised devices.
- Avoid using public or unsecured Wi-Fi unless using a secure VPN.
- Not downloading sensitive data unless strictly necessary and approved.
- Securing your screen from view and locking devices when unattended.
- Using Microsoft 365 platforms (e.g. SharePoint, Teams) for collaboration, not personal drives or Email.

Remote working is a privilege and must not compromise data security.

Handling and Storing Special Category Data

Special category and sensitive data (e.g. safeguarding records, medical information, ethnicity or sexual orientation disclosures) require additional safeguards:

- Access is restricted to designated staff on a strict need-to-know basis.
- Storage must be encrypted or access-controlled, never left in shared drives or paper files without protection.
- Transmission must be secure, and documents must be clearly marked as "Confidential".
- Retention must follow a defined schedule, with regular review for relevance and accuracy.

Special category data must never be stored casually, printed unnecessarily, or discussed in open spaces.

Retention, Disposal, and Redundancy

SLP College only retains personal data for as long as it is needed to meet its original purpose or legal obligation. When it is no longer required, it must be securely disposed of.

- **Paper records:** must be shredded or placed in designated confidential waste bins.
- **Digital files:** must be permanently deleted, not just moved to the recycle bin.

- **Devices:** must be securely wiped using College-approved methods before reuse or disposal.
- **Cloud storage:** retention must be actively managed, and redundant folders should not accumulate.

The DPO maintains a Data Retention Schedule, and staff are responsible for acting on it locally.

Personal Devices and BYOD

Staff and associates must not use personal devices for processing identifiable student or staff data unless:

- IT and the DPO have granted explicit authorisation.
- The device meets security standards (e.g. encryption, PIN lock, secure login).
- Only College systems (e.g. Microsoft 365) are used for access, not personal Email or drives.
- The user agrees to the College's control over the device if compromised or lost (e.g. remote wipe).

Use of unauthorised personal devices for data processing is prohibited.

Responding to Data Security Incidents

If you know or suspect that personal data has been accessed, altered, lost, or shared without permission, you must:

- Report it immediately to the Data Protection Officer.
- Do not delete or conceal the incident; preserve the evidence.
- Cooperate fully with containment and investigation procedures.

Examples include:

- Sending a report to the wrong person.
- Losing a College laptop or USB.
- Accidentally exposing data through incorrect permissions.
- Discovering a compromised email account.

All incidents must be reported within hours, not days. Early reporting is crucial to mitigate risk and fulfil the College's duty to report serious breaches to the Information Commissioner's Office (ICO) within 72 hours, if required.

Training and Cultural Awareness

All staff must complete mandatory data protection and cybersecurity training on induction and at regular intervals thereafter. Training covers:

- Common risks (e.g. phishing, misdelivery, weak passwords).
- Secure use of College systems.
- Incident reporting procedures.
- Role-specific responsibilities for data handling.

The DPO provides targeted briefings, updates, and resources tailored to emerging threats and role changes.

Continuous Review and Improvement

The College's security arrangements are subject to:

- Annual review by the DPO and SLT.
- Internal and external audits.
- Real-time review after any breach, near miss, or ICO advice.
- Monitoring of national and sector alerts (e.g. NCSC, Jisc, OfS).

10. Data Protection by Design and Default

At SLP College, we do not treat data protection as a compliance afterthought. We build it from the beginning. Our commitment to data protection by design and by default means that privacy is embedded into the planning, development, and delivery of every system, service, and process that involves personal data.

This approach is not just a legal requirement under Article 25 of the UK GDPR; it reflects our institutional values of trust, accountability, and professionalism.

What It Means in Practice

Data protection by design requires us to:

- Anticipate risks to personal data before they arise.
- Integrate privacy-enhancing features into systems, tools, and processes from the outset.
- Consult the right people, particularly the Data Protection Officer (DPO), at the planning stage.
- Test, monitor, and review privacy controls regularly.

Data protection by default means that:

- We only collect the minimum personal data needed for a clear, lawful purpose.
- Access is automatically restricted to those who need it.
- Data is not kept for longer than necessary.
- Privacy settings are switched "on" by default (e.g. visibility, sharing, retention).

This applies across all contexts, admissions forms, video recordings, performance systems, safeguarding disclosures, third-party platforms, assessment workflows, and more.

When the Principle Applies

You must apply data protection by design and default whenever:

- Creating or revising a form, platform, or digital system.
- Designing or delivering a new programme, module, or pastoral service.
- Integrating a new supplier, cloud system, or student support tool.
- Initiating a research project, outreach activity, or student engagement campaign.
- Handling special category data (e.g. health, ethnicity, neurodiversity, safeguarding).
- Recording, streaming, photographing, or publishing student or staff content.

If your work involves personal data, these principles apply, even if you are not the one building the system or collecting the information.

Data Protection Impact Assessments (DPIAs)

Where a proposed activity is likely to result in a high risk to individuals' rights or freedoms, a Data Protection Impact Assessment (DPIA) is legally required. DPIAs must be completed before any data is collected or the system is launched.

Triggers for a DPIA include:

- Large-scale or ongoing collection of special category data.
- Use of new or unfamiliar technologies (e.g. facial recognition, automated profiling).
- Systematic monitoring or observation of individuals (e.g. attendance tracking, logging interactions).
- Data sharing with external partners, including universities, agents, or vendors.
- Activities involving vulnerable groups (e.g. safeguarding, counselling, minors).
- Video or audio capture of identifiable individuals for reuse outside the College.

A DPIA must:

- Describe the purpose and scope of the processing.
- Assess the necessity and proportionality of the data being used.
- Identify potential risks to individuals' rights.
- Propose measures to eliminate or reduce those risks.
- Be reviewed and approved by the DPO, with escalation to SLT if necessary.

SLP College maintains a central DPIA Register and reviews outcomes as part of audit and assurance cycles.

Roles and Responsibilities

Role	Responsibility
System owner / Project lead	Identify risks early, engage the DPO, complete DPIAs, and implement controls.
Data Protection Officer (DPO)	Advise on compliance, review DPIAs, monitor risk, and challenge poor design decisions.
IT and Procurement Teams	Ensure technical controls and contracts meet College and legal standards.
All staff and associates	Ask early, involve the DPO, never assume privacy is someone else's job.

If you are unsure whether a DPIA is needed or what controls are appropriate, ask the DPO before proceeding.

Real-World Examples

Scenario	Privacy by Design and Default in Action
Launching a new student support referral form	Collect only essential details; access is restricted to the Support team; retention is 12 months.
Filming end-of-term performances	Explicit consent obtained; access restricted to marketing team; withdrawal honoured
Trialling a third-party mental health app	DPIA conducted; supplier contract reviewed; anonymised uptake analytics used only
Rebuilding the admissions database	Old data purged; fields rationalised; applicant access included for transparency.
Creating a safeguarding incident log	Protected by encryption, audit log enabled; retention controlled by risk categorisation.

These examples demonstrate that privacy is not a barrier to innovation; it's a mark of institutional competence.

Oversight and Continuous Improvement

The DPO ensures that:

- All high-risk processing is subject to DPIA review.
- New systems, tools, or partnerships are assessed for compliance readiness.
- Feedback loops are built into project closure or post-implementation review.
- Lessons from audits, breaches, or sector incidents inform future design choices.

SLP College maintains a privacy-by-design assurance framework, reviewed annually by the SLT, to ensure continuous alignment with legislation, student trust, and operational reality.

Our Cultural Commitment

At SLP College, data protection by design and default reflects the same care and forethought we apply to curriculum planning, student support, and artistic integrity. It signals to students, staff, and the wider public that we take privacy seriously and that we build our systems around people, not the other way around.

We do not ask, "What can we collect?"

We ask, "What do we really need—and how do we protect it?"

This mindset is embedded across our operations and is central to our identity as a modern, student-centred, professionally accountable conservatoire.

11. Data Protection Impact Assessments (DPIAs)

At SLP College, we use Data Protection Impact Assessments (DPIAs) to anticipate, assess, and reduce risks to individuals' privacy. DPIAs are a legal requirement under Article 35 of the UK General Data Protection Regulation (UK GDPR) where processing is likely to result in a high risk to people's rights and freedoms.

However, for us, DPIAs are more than a compliance mechanism; they are a marker of foresight, maturity, and professional respect for the people whose data we process.

When a DPIA Is Required

You must carry out a DPIA before any processing begins if the activity is likely to be high risk. This includes, but is not limited to:

- Processing large volumes of special category data (e.g. health, ethnicity, safeguarding).
- Monitoring individuals (e.g. attendance logs, analytics tools, behavioural tracking).
- Recording or publishing identifiable content (e.g. performances, rehearsals, class footage).
- Using new or unfamiliar technology (e.g. biometrics, AI, location tracking).
- Introducing or significantly changing digital systems or cloud services.
- Sharing data with new partners or third parties, particularly cross-border.
- Profiling or automated decision-making about students, staff, or applicants.
- Processing data about vulnerable individuals or sensitive contexts (e.g. mental health disclosures, parental separation, social services involvement).

If in doubt, ask the DPO before proceeding. You cannot complete a DPIA after the fact.

Who Is Responsible

Role	Responsibility
Project lead/system owner	Initiates and completes the DPIA using the College template; owns the risks and mitigation plan.
Data Protection Officer (DPO)	Advises on approach, challenges assumptions, approves or rejects DPIAs, and escalates as needed.
IT / Procurement / Safeguarding	Provide specialist input on technical design, supplier security, legal obligations, or welfare risks.
Senior Leadership Team (SLT)	Oversees institutional risk, prioritises mitigation, and authorises high-impact or high-exposure projects

The DPO maintains the College DPIA Register and ensures timely review, follow-up, and escalation.

What a DPIA Must Cover

All DPIAs must use the College-approved template and include:

- **A clear description of the activity.**
  - What data is collected?
  - Who is affected and in what ways?
  - How will the data be used, accessed, and stored?
- **The legal basis for processing.**
  - What Article 6 and (if relevant) Article 9 bases apply?
  - Does the project involve consent, a public task, or substantial public interest?
- **An assessment of proportionality.**
  - Is this the least intrusive way to achieve the intended purpose?
  - Are you collecting more than you need?
  - Have alternatives or mitigations been considered?
- **An assessment of risks.**
  - What could go wrong, and for whom?
  - What is the likelihood and severity of harm?
  - Are there group-based risks (e.g. discrimination, exclusion, misrepresentation)?
- **Measures to reduce or eliminate those risks.**
  - Technical (e.g. encryption, access controls, deletion triggers).
  - Organisational (e.g. restricted teams, training, supervision).
  - Legal (e.g. contracts, safeguarding procedures, opt-outs).
- **Consultation.**
  - Has the DPO been involved from the start?.
  - Have students, staff, or affected groups been consulted (where appropriate)?
  - Have suppliers, safeguarding leads, or external partners reviewed the plan?
- **DPO opinion and sign-off.**
  - Is the DPIA complete and lawful?

- Are the risks acceptable or manageable?
- Should the project proceed, be amended, or escalated?

DPIA Outcomes and Follow-Up

Once a DPIA is approved, the project lead is responsible for:

- Implementing the controls and safeguards as agreed.
- Monitoring for unintended consequences or new risks.
- Reviewing the DPIA if the scope, system, or data changes.
- Updating the DPO if incidents or breaches occur.

If a project presents high risk that cannot be mitigated, the DPO must consult the Information Commissioner's Office (ICO) before any processing begins. This is a legal requirement under UK GDPR Article 36.

Common DPIA Misconceptions, Corrected

Myth	Reality
"It's just a form to tick off."	No, it's a legal, risk-based decision process that may prevent harm or reputational damage.
"It only applies to IT systems."	Wrong, DPIAs also apply to forms, data sharing, events, and physical records.
"We can do the DPIA after launch."	Not allowed. DPIAs must be completed and signed off on before any processing starts.
"The DPO writes the DPIA."	Incorrect, the project lead owns the DPIA; the DPO reviews and advises.

DPIAs and Institutional Trust

DPIAs are how we demonstrate to students, staff, alumni, and regulators that:

- We respect the right to privacy and autonomy.
- We make thoughtful, ethical decisions about data.
- We recognise power dynamics and strive to minimise risk.
- We anticipate, not react to, problems.
- We document our decisions and stand by them.

Each DPIA is part of our professional contract with the people we serve.

Where to Access Support

You can access:

- The College DPIA template is available on the staff intranet or via the DPO.
- Guidance from the DPO on DPIA triggers, completion, and escalation.

- Input from safeguarding, IT, estates, marketing, or programme leads, depending on context.
- Examples of anonymised past DPIAs (where appropriate) for benchmarking.

Always build time into project planning for DPIA review and DPO consultation. DPIAs are fast to do properly, and slow to fix when missed.

12. Personal Data Breaches

At SLP College, we recognise that a personal data breach is not just a technical failure; it is a breach of trust. Our response must be immediate, proportionate, and accountable.

We maintain a zero-tolerance culture toward silence, delay, or concealment. This section outlines how we identify, report, investigate, and respond to any incident involving personal data loss, misuse, or exposure, no matter how minor it may first appear.

What Constitutes a Personal Data Breach

A personal data breach is any event, accidental or deliberate, that compromises the:

- Confidentiality (unauthorised access or disclosure).
- Integrity (unauthorised alteration or corruption).
- Availability (unauthorised loss, deletion, or inaccessibility).

of personal data. This includes breaches involving:

- Paper files.
- Emails and digital systems.
- Voicemail, messaging apps, or verbal disclosures.
- Cloud services or third-party platforms.

Examples include:

- Sending student data to the wrong recipient.
- Misplacing safeguarding notes or assessment results.
- Allowing unauthorised access to staff files.
- Publishing identifiable content without consent.
- Losing an unencrypted laptop or USB stick.
- System failures that block timely access to critical data.

Breaches are assessed based on risk, not just intent or outcome. An incident involving sensitive data (e.g. health or safeguarding records) may be serious even if detected quickly.

Immediate Action: What You Must Do

If you suspect or know a breach has occurred:

1. Immediately report it to the Data Protection Officer (DPO).
    - Do not delay while checking or seeking approval.
    - Use phone, Email, or in-person notification, whatever is fastest.
2. Do not attempt to erase or fix the problem without guidance.
    - Preserve the evidence.
    - Do not delete emails, logs, or files unless instructed.
3. Contain the breach if safely possible.
    - For example, recall the Email, change passwords, and restrict access.

The priority is to prevent further harm, not assign blame. Our institutional approach is "report fast, not perfect."

Who Must Report

Everyone. All staff, freelancers, contractors, and associates have a legal and contractual duty to report any data breach or suspected breach.

Never assume someone else is handling it. Never delay "just to be sure."

If you are not sure whether something is a breach, report it anyway. The DPO will advise.

DPO-Led Breach Response

The Data Protection Officer coordinates breach management. Upon receiving a report, the DPO will:

- Log the incident in the College Data Breach Register.
- Assess the severity and scope using a standardised risk matrix.
- Initiate containment actions in collaboration with IT, safeguarding, or leadership as appropriate.
- Determine whether notification is required, internally, to data subjects, or the Information Commissioner's Office (ICO).
- Oversee communication, remediation, and review.

Serious or repeated breaches are escalated to the Senior Leadership Team (SLT) and included in annual governance reporting.

When the ICO Must Be Notified

The College must report a breach to the ICO within 72 hours if it is likely to result in a risk to the rights and freedoms of individuals, such as:

- Identity theft.
- Financial loss.
- Discrimination.
- Emotional distress or reputational harm.
- Loss of access to vital services.

Only the DPO (or, if delegated, a member of SLT) may formally notify the ICO. Reports include:

- What happened.
- How many people were affected.
- The types of data involved.
- Mitigation steps already taken.
- Plans to reduce further risk.
- Contact details for follow-up.

If a breach is not reported, the reasons must be documented.

Notifying Affected Individuals

Where a breach poses a high risk to individuals, SLP College will notify them directly unless:

- It would cause greater harm (e.g. a safeguarding risk).
- It is impractical (e.g. lost data with no identifiable link).
- Effective mitigation (e.g. encryption) makes notification unnecessary.

Notifications are:

- Written in plain English.
- Sent securely.
- Include what happened, what data was involved, how we're responding, and what the individual can do.

Where direct contact is not possible, we will issue a public statement or post a notice on relevant platforms.

Breach Classification and Examples

Risk Level	Example Incident	Likely Action
Low	An email with a non-sensitive timetable was sent to the wrong internal recipient.	Logged, team reminder issued.
Moderate	Assessment data was shared with the wrong student cohort.	Logged, contained, students informed, and reviewed.

High	Lost safeguarding folder or medical disclosure leaked externally	The ICO was notified, individuals were informed, and SLT was briefed.
Critical	Ransomware attack compromises core systems and sensitive data	ICO + legal notification, and the cyber incident protocol was activated.

Every breach is logged and reviewed, even if minor or rapidly contained.

Cyber and System Breaches

SLP College maintains cyber insurance and access to external incident response specialists.

The DPO, in collaboration with IT and SLT, will activate the Cyber Incident Response Plan if:

- There is evidence of malware, ransomware, or unauthorised intrusion.
- Cloud platforms are compromised.
- Student or staff login credentials are stolen.
- Systems storing special category data are impacted.

This includes:

- Immediate forensic containment.
- Communications with suppliers and regulators.
- Business continuity planning.
- Post-incident remediation and reporting.

Post-Breach Review and Continuous Improvement

Every breach is followed by a review to ensure lessons are learned. The DPO will:

- Identify root causes and contributing factors.
- Recommend changes to systems, policies, or training.
- Coordinate actions with team leads.
- Share anonymised findings as part of internal learning.

Persistent or repeated breaches in a department or process may trigger a formal audit or compliance review.

A No-Blame, Report-First Culture

We do not punish honest mistakes that are reported quickly. We do take action against:

- Failing to report a breach.
- Deliberate concealment.
- Negligent repeat behaviour after guidance has been issued.

We want breaches reported early, even if they turn out to be low risk, because our ability to contain, notify, and support depends on speed.

If you have to ask, “Should I report this?”, you should.

A breach is not a moment of failure; it is a moment of responsibility. At SLP College, we respond with speed, care, and clarity to protect the people we serve and the values we stand for.

13. Training, Monitoring, and Compliance Assurance

At SLP College, we take a proactive, whole-institution approach to data protection. We do not rely on policy documents alone. Instead, we embed privacy awareness, accountability, and professional discipline into how we train our people, monitor our systems, and assure our compliance.

This section sets out how we ensure that data protection is understood, implemented, and continuously improved across the College. Compliance is not a one-off action; it is a standard of behaviour, reinforced by evidence and oversight.

Staff Training

All staff, visiting professionals, and contractors who process personal data must complete mandatory data protection training. This includes:

- **Induction training:** on or before the first day of access to College systems or data.
- **Refresher training:** at least every two years, or earlier if triggered by system changes, role changes, policy updates, or data incidents.
- **Role-specific sessions:** for staff involved in high-risk or high-volume processing (e.g. Admissions, Safeguarding, Registry, HR, Marketing, IT, Digital Media)

Training covers:

- UK GDPR principles and lawful bases.
- Recognising and reporting data breaches.
- Handling special categories and safeguarding data.
- Consent, retention, and sharing protocols.
- Subject access and individual rights.
- Privacy by design, DPIAs, and working with suppliers.

Delivery includes live briefings, digital modules, and scenario-based exercises relevant to a conservatoire setting.

Completion is mandatory. Records are held centrally and reported to SLT quarterly.

Student and Public Awareness

We ensure students, alumni, and the wider community are informed of their rights and our responsibilities through:

- Clear, accessible privacy notices at the point of data collection.
- Induction briefings for new students.
- Data protection content in digital safety, safeguarding, and student support workshops.
- Consent processes for performance recording, marketing, and research participation.
- Transparent forms and opt-out options for marketing communications and alumni engagement

Where students are under 18 at the point of entry, we include age-appropriate guidance and, where lawful, engage parents or carers in consent and safeguarding disclosures.

Monitoring and Internal Assurance

The College operates a structured monitoring framework to test, validate, and continuously improve compliance:

Activity	**Frequency**	**Led By**
Data Protection Audit	Annually	DPO
Training Compliance Review	Quarterly	DPO / HR
Thematic Spot Checks	Termly	DPO / IT / Department Leads
Post-Breach Review	Within 10 working days	DPO / Line Manager
DPIA Register and Risk Review	Ongoing; summary quarterly	DPO

These findings are:

- Documented in full.
- Tracked until resolved.
- Escalated to SLT or Directors where systemic issues or repeat patterns are found.

Departmental Responsibility

While the DPO leads on compliance strategy, day-to-day responsibility rests with line managers and department heads.

They must ensure:

- Staff are trained and retrained when roles or risks change.
- Privacy is embedded in planning, procurement, and communication.
- DPIAs are initiated where needed.

- Access to systems and data is appropriate and reviewed regularly.
- Records are accurate, necessary, and deleted when no longer required.

Every manager is accountable for the compliance standards of their team.

Escalation and Enforcement

SLP College operates a proportionate but firm approach to enforcement. Failure to comply with data protection training or procedures may result in:

- Mandatory retraining.
- Access restrictions to College systems.
- Disciplinary investigation.
- Contractual review (for freelancers and suppliers).

Deliberate or reckless non-compliance, particularly involving sensitive or safeguarding data, will be treated as gross misconduct and may result in dismissal or legal referral.

Oversight by SLT and Regulatory Readiness

The Data Protection Officer provides quarterly updates to the Senior Leadership Team, including:

- Breach log and response trends.
- DPIA activity.
- Training completion rates.
- Supplier compliance risks.
- Audit outcomes and remedial actions.
- Regulatory guidance updates (ICO, OfS, Ofsted, UKVI).

This ensures institutional readiness for:

- OfS registration and condition B2 (management and governance).
- Ofsted inspection of safeguarding and records handling.
- ICO breach investigations or subject access complaints.
- UKVI sponsor compliance checks.
- Professional indemnity and cyber insurance renewals.

Continuous Improvement and Sector Learning

SLP College does not wait for breaches to review its processes. We actively improve compliance through:

- Policy reviews every 12 months (or sooner if law or risk changes).
- Staff feedback loops on forms, processes, and training.

- Learning from anonymised breaches (internal and sector-wide).
- Use of ICO case studies, NCSC alerts, and peer benchmarking.
- Integration of data protection questions into project reviews and evaluation cycles.

Privacy is not a static obligation; it evolves as systems, relationships, and risks change. Our policy framework is designed to be living, responsive, and institutionally owned.

Our Cultural Standard

We do not train staff to avoid mistakes. We train staff to understand risk, recognise red flags, and act with integrity. Our monitoring is not about control, it's about assurance. Our compliance isn't box-ticking, it's behavioural.

At SLP College, protecting personal data is a shared discipline. It reflects our standards, our culture, and our commitment to every individual who entrusts us with their information.

14. Linked Policies and Governance Documents

Data protection is not an isolated legal duty; it is an embedded standard across all areas of institutional life at SLP College. This section sets out the key policies, procedures, and governance documents that support, reinforce, or intersect with this Data Protection Policy.

Together, they form a coherent policy environment that ensures every use of personal data is lawful, proportionate, and institutionally accountable.

Supporting Policies and Procedures

The following internal policies provide detailed operational guidance aligned with this Data Protection Policy. They are reviewed annually by the policy owner and approved by the Senior Leadership Team (SLT).

Policy/Procedure	**Purpose and Link to Data Protection**
Privacy Notices (All Data Subjects)	Clearly inform individuals how and why their data is collected, used, shared, and stored.
Records Retention and Disposal Policy.	Defines how long data is kept and how it is securely deleted or destroyed.
Information Security Policy	Sets technical and organisational safeguards for systems, devices, and access controls.
Data Breach Response Procedure	Establishes reporting lines, investigation protocols, and ICO notification requirements.
IT Acceptable Use Policy	Governs responsible digital behaviour and secure use of College systems.
Safeguarding Policy	Governs lawful information sharing where there is risk to a child or vulnerable adult.
CCTV Policy	Ensures lawful, proportionate, and clearly communicated use of surveillance technology.

Photography, Filming, and Audio Policy	Provides lawful bases and consent protocols for capturing and using identifiable media.
Freedom of Information (FOI) Policy	Supports transparency while protecting personal data through lawful exemptions
Complaints Procedures	Covers data subject complaints related to access rights or perceived misuse of data

All policies are version-controlled, legally reviewed, and available to staff via the internal policy library. Student-facing versions use accessible language and are distributed at the point of relevance (e.g. enrolment, audition, induction) and are available on the SLP College website.

Legal and Regulatory Frameworks Referenced

This policy is grounded in and interprets the following statutory frameworks:

Legislation/Framework	**Application**
UK General Data Protection Regulation (UK GDPR)	Core regulatory standard for all personal data processing.
Data Protection Act 2018	Governs special category and criminal offence data, exemptions, and UK-specific duties.
Privacy and Electronic Communications Regulations (PECR)	Regulates marketing communications and website tracking (cookies, Email, SMS).
OfS Conditions of Registration (esp. B2)	Requires effective governance of student records and institutional compliance systems.
Ofsted Inspection Framework	Requires secure, lawful handling of safeguarding and learner records.
UKVI Sponsor Guidance	Requires accurate, timely reporting of international student data.
Information Commissioner's Office (ICO) Codes	Interprets legal standards on data sharing, individual rights, and accountability
Photography, Filming, and Audio Policy	Provides lawful bases and consent protocols for capturing and using identifiable media.
Freedom of Information (FOI) Policy	Supports transparency while protecting personal data through lawful exemptions
Complaints Procedures	Covers data subject complaints related to access rights or perceived misuse of data.

These frameworks are monitored continuously by the DPO and referenced in DPIAs, policy reviews, and internal audits.

Oversight and Integration

This Data Protection Policy is formally owned by the Senior Leadership Team (SLT) and operationally led by the Data Protection Officer (DPO). It is fully integrated with:

- Governance reporting cycles (e.g. breach logs, DPIA summaries, SLT dashboards).
- External compliance (e.g. OfS, Ofsted, UKVI, ICO inspections or self-reporting).
- Procurement and due diligence (e.g. third-party data processors, EdTech, cloud services).
- Staff lifecycle processes (e.g. recruitment, performance, safeguarding).

- Student lifecycle processes (e.g. application, enrolment, assessment, alumni engagement).

This policy is not standalone; it functions within a structured policy map reviewed and approved annually by the SLT.

Policy Hierarchy and Conflict Resolution

In the event of conflicting instructions between policies:

- The Safeguarding Policy takes operational precedence in welfare and protection matters.
- The Data Protection Policy governs where privacy rights or legal bases for processing are in question.

The DPO may be consulted to interpret the interaction between overlapping duties (e.g. legal obligation vs. consent)

Conflicts between internal policies must be resolved through legal and operational alignment, not parallel interpretation. The DPO is the final institutional authority on the lawful processing of personal data.

Cross-Referencing and Policy Access

To ensure transparency and staff usability:

- All linked policies are published on the internal policy portal and referenced in relevant staff and student handbooks.
- Student-facing versions are drafted in plain English and reviewed for accessibility.
- Contracts and partner agreements explicitly reference this policy where data sharing is involved.
- DPIAs, breach logs, and internal audits cross-reference applicable linked policies for accountability

Staff are responsible for knowing which policies apply to their role. Managers must ensure teams receive role-specific briefings as part of local induction and ongoing professional development.

Institutional Commitment

This Data Protection Policy is a framework for trust. Its strength depends on how well it is supported, interpreted, and enforced through every other policy, contract, and behaviour across the College.

At SLP College, every policy that touches personal data must be lawful.

Every team must be accountable. Every system must be secure. Every decision must reflect our values.

That is what governance means in practice.

15. Policy Review and Updates

SLP College maintains this Data Protection Policy as a living institutional document, governed by rigour, reviewed with discipline, and updated in response to law, risk, and operational reality.

This section sets out how the policy is maintained, who is responsible for its currency, and how changes are governed, communicated, and embedded.

Governance, Ownership, and Authority

This policy is owned by the Senior Leadership Team (SLT), which acts as the governing body of SLP College and the legal Data Controller under UK GDPR.

The Data Protection Officer (DPO) is the operational lead responsible for:

- Coordinating annual and interim reviews.
- Consulting with relevant internal and external stakeholders.
- Monitoring changes in law, regulation, and best practice.
- Proposing amendments, with justification and risk rationale.
- Ensuring alignment with linked policies, contracts, and compliance registers.
- Reporting outcomes and recommendations to SLT.

No changes to this policy may be made without SLT approval. All version changes are logged and retained for audit.

Scheduled Review Cycle

This policy is reviewed at least annually. The DPO initiates the review three months before expiry to allow time for:

- Legal checks.
- Cross-policy harmonisation.
- SLT consideration.
- Communication and staff briefing.

The review cycle ensures this policy remains:

- Legally compliant (UK GDPR, DPA 2018, PECR).
- Regulator-ready (OfS, Ofsted, UKVI, ICO).
- Operationally accurate.
- Proportionate to institutional scale and risk.

Early or Interim Reviews

In addition to the annual cycle, the policy is reviewed immediately following any of the following triggers:

Trigger	Response
Major legal or regulatory change (e.g. ICO guidance)	Review and align within 30 days of publication.
Serious data breach or ICO investigation.	Full post-incident policy review, including lessons learned.
New core system or data platform.	Update scope, definitions, and DPIA references.
Change in SLT governance or DPO appointment.	Confirm continuity of oversight and authority.
Audit or external review finding.	Implement corrective action and integrate it into the policy.
Reputational risk or legal dispute involving data.	Conduct targeted section review, escalate to full policy review if needed.

All interim reviews are recorded in the version control log and referenced in the DPO's quarterly report to SLT.

Cross-Policy Coordination

The DPO ensures that this policy is harmonised with:

- Safeguarding, IT, and HR policies.
- Records retention schedules.
- Privacy notices and consent mechanisms.
- DPIA processes.
- Breach response protocols.
- Supplier contract templates and due diligence workflows.

If a change in one document affects others, the DPO leads a coordinated update to maintain integrity across all linked frameworks.

Escalation and Regulatory Interface

If at any point:

- The College cannot comply with this policy due to a system, contract, or process gap.
- A proposed activity conflicts with its principles.
- A regulator (e.g. ICO, OfS, UKVI) issues guidance requiring immediate action.

… the DPO must escalate the issue to SLT with a proposed resolution path and legal risk assessment. No derogation from this policy is permitted without SLT and (where applicable) legal approval.