GDPR Policy 2027

Original Policy Date: **27th March 2026**
Revision Date: **5th November 2026**
Policy Responsibility: **Sam Gibbs (Principal)**
Updated or reviewed: **Annually**

Version: ***2.0***
Next Scheduled Review: ***November 2027***

PERFORMERS THEATRE COMPANY

INTRODUCTION

Performers Theatre Company is committed to protecting the personal information of its students, parents, carers, staff, volunteers and other individuals whose information it collects or processes.

We recognise that much of the information entrusted to us relates to children and young people, including medical information, emergency contacts and safeguarding concerns. We take our responsibilities for protecting this information seriously.

Performers Theatre Company acts as a Data Controller for the personal information it determines how and why to process. This means we are responsible for ensuring that personal information is collected, used, stored, shared and disposed of appropriately.

We process personal data in accordance with applicable UK data protection legislation, including:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018, as amended.
- The Privacy and Electronic Communications Regulations 2003 (PECR), where applicable.
- Other relevant legislation governing the protection and disclosure of personal information.

This policy applies to all employees, freelance teachers, volunteers, visiting professionals and other individuals who process personal data on behalf of Performers Theatre Company.

Data Protection Lead: Sam Gibbs, Principal
Contact: admin@performerstheatrecompany.com

The Principal is responsible for overseeing compliance with this policy. This internal designation does not imply that the organisation has appointed a statutory Data Protection Officer.

DATA PROTECTION PRINCIPLES

Performers Theatre Company follows the seven core principles of UK GDPR.

Personal data must be:

1. Processed lawfully, fairly and transparently - individuals must understand how their information is used.
2. Collected for specified, explicit and legitimate purposes - information must not be used for incompatible purposes.
3. Adequate, relevant and limited to what is necessary - only essential information should be collected.
4. Accurate and kept up to date - incorrect information should be corrected promptly.
5. Kept for no longer than necessary - retention periods must be appropriate to the information and its purpose.
6. Processed securely - appropriate measures must protect information from loss, misuse, unauthorised access or disclosure.
7. Subject to accountability - Performers must be able to demonstrate compliance with these principles.

All staff are expected to apply these principles when handling personal information.

PERSONAL INFORMATION WE COLLECT

Performers Theatre Company collects and processes information necessary for the safe, effective and lawful operation of its classes, productions and activities.

Students and Families

Information may include:

- Student's full name and date of birth.
- Home address and relevant contact information.
- Parent or carer names, telephone numbers and email addresses.
- Emergency contact details.

- Enrolment and attendance records.
- Class, workshop and production participation.
- Medical information, allergies and relevant health conditions.
- Special educational needs, disabilities and reasonable adjustment requirements.
- Relevant safeguarding and welfare information.
- Photograph, video and publicity permissions.
- Payment, invoice and account information.
- Performance licensing and chaperone-related information where required.

Parents and carers are responsible for notifying Performers of relevant changes to the information they have supplied.

Staff, Freelancers and Volunteers

Information may include:

- Full name, address and contact details.
- Date of birth where necessary.
- Employment, engagement and contractual information.
- National Insurance and payroll information where applicable.
- Bank details and payment records.
- Identification and right-to-work documentation.
- Relevant qualifications, training and professional experience.
- DBS eligibility, verification and checking information.
- Safeguarding training and suitability records.
- Relevant employment, conduct and disciplinary information.

Information is collected only where necessary and is subject to appropriate confidentiality and retention arrangements.

Other Individuals

Performers may also process information relating to:

- Customers purchasing tickets or attending events.
- Workshop and masterclass participants.
- Visitors and contractors.
- Suppliers and professional advisers.
- Individuals making enquiries, complaints or requests.

LAWFUL BASIS FOR PROCESSING

Performers Theatre Company will identify an appropriate lawful basis before processing personal information.

Depending on the purpose, these may include:
Consent: Where an individual has freely agreed to a specific use of their information, such as optional promotional photographs or certain marketing communications.
Contract: Where processing is necessary to provide an agreed service, administer enrolment or manage contractual arrangements.
Legal Obligation: Where information must be processed to meet applicable legal requirements, including certain employment, taxation, safeguarding or performance licensing obligations.
Legitimate Interests: Where processing is necessary for a legitimate organisational purpose and is not overridden by the rights and interests of the individual, particularly where children are concerned.
Vital Interests: In exceptional circumstances where processing is necessary to protect someone's life.

Where personal information includes special category data, such as health information, Performers must also identify and document an applicable condition under Article 9 UK GDPR and, where relevant, the Data Protection Act 2018.

Criminal offence information, including relevant DBS-related information, must only be processed where legally authorised and subject to appropriate safeguards.

Consent is not the lawful basis for every activity. For example, information may need to be shared with appropriate safeguarding authorities without consent where a lawful basis and relevant conditions permit or require this.

CHILDREN'S INFORMATION AND SAFEGUARDING

Performers Theatre Company recognises that children require particular protection when their personal information is processed.

Information relating to children must be handled carefully, proportionately and only for legitimate purposes.

Safeguarding Information

Safeguarding information must be:

- Recorded accurately and factually.
- Shared only with individuals or agencies who have a legitimate need to know.
- Stored separately from routine administrative records wherever appropriate.
- Accessible only to appropriately authorised individuals.
- Retained in accordance with applicable safeguarding requirements and the organisation's retention schedule.

The Designated Safeguarding Lead (DSL) is responsible for overseeing safeguarding information handling in conjunction with the organisation's safeguarding procedures.

Designated Safeguarding Lead: Sam Gibbs
Deputy Designated Safeguarding Lead: Jess Eaton

Safeguarding information may be shared with relevant statutory agencies where necessary and lawful to protect a child or fulfil safeguarding responsibilities.

Consent is not always required before making an appropriate safeguarding referral.

Medical and Additional Support Information

Medical information and details of additional support requirements must be handled confidentially.

Access will be restricted to authorised individuals who require the information to support a student's safety, wellbeing or participation.

Relevant information must remain promptly accessible to authorised staff during an emergency.

Staff must not disclose medical or additional support information to other families, students or unauthorised individuals.

DATA STORAGE, ACCESS AND SECURITY

Performers Theatre Company uses electronic and, where necessary, paper-based systems to administer its activities.

Appropriate technical and organisational measures must be maintained to protect personal information.

ClassManager

ClassManager is used to manage student enrolment, parent and carer contact details, attendance, invoicing and other administrative information.

Access to ClassManager is restricted to authorised members of staff.

Permissions must reflect individual responsibilities, and staff must only access information necessary for their duties.

Medical details and emergency contact information must remain available to appropriately authorised staff when needed for student safety.

Access permissions must be reviewed when responsibilities change or an individual leaves the organisation.

Google Drive and Electronic Records
Google Drive is used for authorised organisational administration and record keeping.

Confidential information must be stored in appropriately restricted folders.

The organisation's central Incident Log may be accessed only by authorised staff.

Safeguarding records, sensitive medical information and confidential employment information must be subject to additional access restrictions and must not be routinely available to all individuals with access to the general Incident Log.

Sharing permissions must be checked before confidential documents are distributed.

Account and Device Security
Staff handling personal information must:

- Use secure passwords and avoid sharing login credentials.
- Enable multifactor authentication where available and appropriate.
- Keep devices and software reasonably up to date.
- Lock devices when unattended.
- Avoid using unsecured or shared devices to access confidential information.
- Report lost devices, suspicious account activity or unauthorised access promptly.
- Use approved systems and communication methods when handling personal information.

Confidential information must not be downloaded, copied or retained on personal devices unless specifically authorised and appropriately secured.

Paper Records
Where paper records are required, they must be kept securely and accessed only by authorised individuals.

Paper documents containing personal information must not be left unattended in classrooms, rehearsal spaces, public areas or vehicles.

Records must be securely destroyed when no longer required, in accordance with the retention schedule.

Staff Access and Confidentiality
All staff, freelancers and volunteers must maintain confidentiality when handling information obtained through their role.

Personal information must not be accessed out of curiosity, discussed unnecessarily or shared through unauthorised channels.

Access must be withdrawn promptly when an individual's role ends or changes.

Any deliberate or negligent misuse of personal information may result in appropriate disciplinary, contractual or other action.

SHARING PERSONAL INFORMATION

Performers Theatre Company may share personal information where necessary, proportionate and lawful.

Recipients may include:

- Local authorities responsible for child performance licensing.
- Safeguarding agencies and statutory authorities.
- Appropriate chaperones and production personnel.
- DBS processing organisations, including Care Check where used.

- Payroll, accounting and professional service providers.
- ClassManager and other authorised technology providers.
- Venues, theatres and production partners where necessary for an agreed activity.
- Emergency services and healthcare professionals in appropriate circumstances.

Only information necessary for the relevant purpose should be shared.

Where external providers process information on behalf of Performers, appropriate contractual and security arrangements must be in place.

Where information is transferred internationally, Performers must ensure an appropriate lawful transfer mechanism or other applicable safeguard is in place.

Personal information must not be sold or disclosed to third parties for unrelated purposes.

PHOTOGRAPHS, VIDEOS AND AUDIO RECORDINGS

Performers Theatre Company may capture photographs, videos and audio recordings during classes, rehearsals, performances, workshops and other activities.

Such recordings may be used for:
- Educational and rehearsal purposes.
- Internal administration and production review.
- Promotional and marketing activities, where appropriately authorised.
- Production filming and distribution under applicable arrangements.

Photograph and video permissions are recorded through the organisation's registration and consent arrangements.

Where consent is relied upon, it must be appropriately obtained, recorded and capable of withdrawal.

Withdrawal of consent will be respected for future processing that relies on that consent. It may not always be possible to retrieve material already lawfully distributed or published, and other lawful bases may apply to particular recordings.

Staff must check relevant permissions before using identifiable student images for promotional purposes.

Images must not be accompanied by unnecessary identifying information.

Any filming or photography by external providers must be subject to appropriate arrangements concerning permissions, confidentiality, security and permitted use.

This section should be read alongside the organisation's Photographs and Images Policy.

INDIVIDUAL DATA PROTECTION RIGHTS

Individuals have rights under UK GDPR, subject to applicable legal conditions and exemptions.

Right to Be Informed
Individuals have the right to receive clear information about how their personal data is collected and used. Performers will provide appropriate privacy information at relevant points of collection.

Right of Access
Individuals may request access to personal information held about them.

This is commonly known as a Subject Access Request (SAR).

Requests may be made verbally or in writing and must be recognised and handled appropriately.

Performers will normally respond within one calendar month, subject to applicable rules regarding extensions, identity verification and exemptions.

Requests must not be refused solely because information is subject to a legal retention requirement.

Right to Rectification
Individuals may request correction of inaccurate personal information or completion of incomplete information.

Performers will consider and respond to such requests in accordance with applicable legal requirements.

Right to Erasure
Individuals may request deletion of personal information in circumstances where the right applies.

The right is not absolute.

Information may need to be retained where there is a lawful reason, including relevant legal obligations, safeguarding considerations or the establishment, exercise or defence of legal claims.

Right to Restrict Processing
Individuals may request that processing of their personal information is restricted in certain circumstances. Where the right applies, Performers will limit processing in accordance with legal requirements.

Right to Data Portability
Where the relevant legal conditions are met, individuals may request personal data they have provided in a structured, commonly used and machine-readable format, or request transmission to another controller where technically feasible.

This right does not apply to every category of information or every type of data sharing.

Right to Object
Individuals may object to certain processing, including processing based on legitimate interests.

Individuals also have the right to object to direct marketing.

Where a valid objection to direct marketing is received, the relevant processing must cease.

Rights Relating to Automated Decision-Making
Individuals have protections relating to certain solely automated decisions, including profiling, that produce legal or similarly significant effects.

Performers Theatre Company does not ordinarily use solely automated decision-making of this nature.

If such processing is introduced, the organisation will review the applicable requirements before implementation.

Exercising Data Protection Rights
Requests should be directed to:
admin@performerstheatrecompany.com

The Principal will coordinate responses and may seek professional advice where appropriate.

Where a request relates to a child's information, Performers will consider the child's competence, best interests, confidentiality and any relevant parental responsibilities before disclosing information.

Requests and responses must be recorded appropriately.

Individuals who remain dissatisfied may complain to the Information Commissioner's Office (ICO).

DATA RETENTION AND SECURE DISPOSAL

Performers Theatre Company will retain personal information only for as long as necessary for the purposes for which it was collected, including applicable legal, regulatory, safeguarding, contractual and operational requirements.

Different categories of information may require different retention periods.

Records must not be retained indefinitely without justification.

The organisation will maintain a **Data Retention Schedule** identifying:

- The category of information.
- The purpose for which it is held.
- The applicable retention period or review trigger.
- The reason for retention.
- The method of secure disposal.

Where legal claims, safeguarding concerns, investigations or other relevant circumstances require information to be retained for longer, disposal may be suspended where lawful and necessary.

Electronic records must be securely deleted when no longer required, taking account of relevant backup arrangements.

Paper records must be securely shredded or destroyed.

The Principal is responsible for overseeing appropriate retention and disposal arrangements.

DATA BREACH PROCEDURE

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

Examples may include:

- An email containing personal information being sent to the wrong recipient.
- Loss or theft of a device containing personal data.
- Unauthorised access to ClassManager or Google Drive.
- Accidental disclosure of confidential student or staff records.
- Compromise of an email account containing personal information.
- Loss of paper documents containing personal data.

Immediate Reporting

All staff must report an actual or suspected personal data breach to the Principal without undue delay.

Staff must not attempt to conceal a breach or delay reporting while investigating it independently.

Containment

The Principal, supported by relevant personnel where appropriate, will take steps to contain the incident.

These may include:

- Securing affected accounts or devices.
- Changing passwords and revoking compromised access.
- Contacting an unintended recipient to request secure deletion.
- Restricting further disclosure.
- Preserving relevant evidence.
- Seeking appropriate technical or professional assistance.

Risk Assessment

The organisation will assess:

- The nature and volume of information affected.
- Whether children or vulnerable individuals are involved.
- Whether medical, safeguarding, financial or other sensitive information is affected.
- The likelihood of misuse or harm.
- The possible consequences for individuals.
- Measures already taken to reduce the risk.

Reporting to the ICO

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, Performers will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where notification is made after 72 hours, the reasons for the delay must be documented.

Informing Affected Individuals

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay, unless an applicable legal exception applies.

Communications must be clear and explain relevant risks and protective steps.

Breach Recording and Review

All personal data breaches must be documented, including those not requiring notification to the ICO.

Records should include:

- Date and nature of the incident.
- Information and individuals affected.
- Assessment of risks.
- Containment and corrective actions.
- Reporting decisions and reasons.
- Any required notifications.
- Lessons learned and preventative measures.

Confidential breach records must be held securely and separately from routine operational information where appropriate.

STAFF RESPONSIBILITIES AND TRAINING

All individuals handling personal data on behalf of Performers Theatre Company must understand their responsibilities.

Staff must:

- Follow this policy and relevant confidentiality requirements.
- Access information only where authorised.
- Maintain appropriate security.
- Check recipients before sending confidential information.
- Report suspected breaches promptly.
- Avoid sharing unnecessary personal information.
- Cooperate with legitimate data protection requests and investigations.

The Principal will ensure that appropriate guidance and training are provided according to the responsibilities of each role.

Data protection arrangements will be reviewed when systems, staffing or organisational activities change.

WEBSITE, PRIVACY INFORMATION AND COOKIES

Performers Theatre Company operates the website:
www.performerstheatrecompany.com

The organisation will provide appropriate privacy information explaining how personal information submitted through the website is collected and used.

Where cookies or similar technologies are used, appropriate information and consent arrangements must be implemented in accordance with applicable requirements.

Strictly necessary cookies may be treated differently from optional analytics, advertising or similar technologies.

The website may contain links to external organisations.

External websites operate under their own privacy policies, and visitors should review those policies before submitting personal information.

Website terms of use should be maintained separately from this Data Protection Policy where appropriate.

ACCOUNTABILITY AND POLICY REVIEW

The Principal is responsible for overseeing the implementation and review of this policy.

Performers Theatre Company will maintain appropriate records and procedures to demonstrate compliance, including where applicable:

- Privacy information and notices.
- Records of relevant processing activities.
- Data retention arrangements.
- Data sharing and processor agreements.
- Records of data protection incidents and breaches.
- Appropriate security and access controls.
- Records of consent where relied upon.
- Data protection impact assessments where required.

The organisation will review this policy annually or sooner where necessary because of changes to legislation, technology, organisational activities or identified risks.

SUMMARY

Performers Theatre Company is committed to ensuring that personal information is handled lawfully, fairly, securely and transparently.

We will:

- Collect only information necessary for legitimate purposes.
- Protect student, family and staff information.
- Restrict access to authorised individuals.
- Give particular protection to children's and safeguarding information.
- Respect individuals' data protection rights.
- Share information only where lawful and necessary.
- Respond promptly to data breaches.
- Retain information only for appropriate periods.
- Review our systems and procedures regularly.

APPENDIX 1

DATA BREACH RESPONSE CHECKLIST

For use by the Principal or authorised person managing an incident.

Immediate Response

- Record when the incident was discovered.
- Identify what happened and which systems are affected.
- Contain the incident and prevent further disclosure.
- Secure compromised accounts, devices or documents.
- Preserve relevant evidence.
- Identify the types of personal data involved.

Risk Assessment

- Identify whose information may be affected.
- Establish whether children's information is involved.
- Identify any sensitive medical, safeguarding or financial information.
- Assess the likelihood and severity of harm.
- Record the risk assessment and reasons.

Notification

- Determine whether ICO notification is required.
- If required, notify the ICO within the applicable timeframe.
- Determine whether affected individuals must be informed.
- Notify other relevant organisations where legally or contractually necessary.

Follow-Up

- Document the incident and decisions.
- Implement corrective actions.
- Review access permissions and security measures.
- Identify lessons learned.
- Close the incident once appropriate action is complete.

APPENDIX 2

DATA RETENTION AND DISPOSAL SCHEDULE

Purpose

This schedule establishes the periods for which Performers Theatre Company will retain personal information relating to students, families, staff, volunteers and organisational activities.

Its purpose is to ensure that personal information is:

- Retained only for as long as necessary.
- Protected against unauthorised access.
- Available where required for safeguarding, legal, financial or operational purposes.
- Reviewed regularly.
- Securely deleted or destroyed when no longer required.

The periods below distinguish statutory requirements from retention periods adopted by Performers Theatre Company as internal policy.

Where different requirements apply to the same record, the longest applicable justified period will take precedence.

Student and Family Records

Record	Retention Period
Student registration and enrolment records	3 years after leaving
Parent/carer contact details	3 years after leaving where retained as part of enrolment records
Emergency contact details	Remove within 3 months of leaving unless needed for an ongoing matter
Current medical information and allergies	Review on departure; normally remove within 3 months unless further retention is justified
SEND and reasonable adjustment information	Review on departure; normally remove within 3 months unless further retention is justified
Routine class attendance registers	3 years after the relevant academic year
Student withdrawal records	3 years after withdrawal, or longer where necessary for an outstanding contractual dispute
Student behaviour and routine incident records	3 years after the incident or departure, whichever is later, subject to safeguarding considerations

Records relating to serious incidents, safeguarding concerns, accidents or legal proceedings must be retained under the relevant longer period.

Safeguarding and Child Protection Records

Record	Retention Period
Child safeguarding and protection files	Normally until the child's 25th birthday
Child sexual abuse safeguarding records	Normally until the child's 75th birthday, subject to specialist review
Serious safeguarding concerns or investigations	Apply the relevant safeguarding period; extend where necessary
Allegations against staff involving children	Apply a separately assessed retention period informed by applicable safeguarding guidance and the circumstances
Safeguarding referrals and correspondence	Retain with the relevant safeguarding case file

Safeguarding records must be held securely with access restricted to the Designated Safeguarding Lead and other specifically authorised individuals.

The Designated Safeguarding Lead must review safeguarding records before any disposal decision.

Records must not be destroyed while relevant investigations, inquiries, complaints or legal proceedings are ongoing or reasonably anticipated.

Accident, Injury and Health and Safety Records

Record	Retention Period
Routine minor accident and first-aid records	3 years after the incident, subject to review
Significant accidents involving children	Normally until at least the child's 21st birthday; longer where justified
Significant accidents involving adults	Normally 6 years after the incident
RIDDOR records	At least 3 years from the date the record was made, where applicable
Risk assessments	Retain current versions; normally archive superseded assessments for 3 years, longer where relevant to an incident or claim
Fire drills and evacuation records	Normally 3 years
Health and safety investigations	Normally 6 years after closure, or longer where justified

Where an accident involves a potentially serious or long-term injury, the Principal must consider whether an extended retention period is appropriate.

Staff, Freelancer and Volunteer Records

Record	Retention Period
Staff personnel files	Normally 6 years after employment or engagement ends
Freelance contracts and engagement records	Normally 6 years after engagement ends
Volunteer administration records	Normally 3 years after involvement ends
Unsuccessful recruitment applications	Normally 6 months after recruitment concludes
Staff training records	During engagement and normally 6 years after departure where relevant to competence or compliance
Safeguarding training records	During engagement and normally 6 years after departure, unless linked to a safeguarding matter
Staff conduct and disciplinary records	In accordance with their relevance, applicable employment requirements and any safeguarding considerations
Right-to-work check records	Duration of employment and 2 years afterwards, where the statutory employer-checking requirements apply

Staff records must be accessible only to individuals authorised to undertake relevant management, payroll, recruitment or safeguarding responsibilities.

DBS Records

DBS information must be handled in accordance with applicable DBS requirements and guidance.

DBS Certificates and Disclosure Information

DBS certificates and detailed disclosure information must not be routinely copied or retained.

Where temporary retention is necessary for a recruitment or suitability decision, information must be kept securely and normally for no longer than six months after the decision, unless a specific lawful justification supports longer retention.

DBS Checking Register

Performers Theatre Company may retain an appropriate register recording:

- Individual's name.
- Position or role.
- Level and type of check.
- Certificate issue date.
- Certificate reference number.
- Date of verification.
- Relevant suitability decision.

The register will be retained during the individual's engagement and reviewed following departure in accordance with the staff retention arrangements.

Financial and Accounting Records

Record	Retention Period
Sales invoices and payment records	Normally 6 years after the relevant financial year
Purchase invoices and receipts	Normally 6 years after the relevant financial year
VAT records	At least 6 years, subject to applicable exceptions
Company accounting and corporation tax records	Normally 6 years after the relevant accounting period, or longer where required
PAYE and payroll records	At least 3 years after the relevant tax year; longer where other requirements apply
Staff payment and contractual financial records	Normally 6 years after the relevant engagement or accounting period
Production financial records	Normally 6 years after the relevant financial year
Refunds, credits and payment disputes	Normally 6 years after resolution where relevant to financial or contractual records

Financial records must be retained for longer where required by an HMRC investigation, ongoing transaction, legal dispute or other applicable requirement.

The Principal will liaise with the organisation's accountant where necessary.

Productions, Rehearsals and Performance Licensing

Record	Retention Period
Production registration and participation records	Normally 3 years after production
Routine rehearsal attendance records	Normally 3 years after production
Child performance licensing records specified by the 2014 Regulations	At least 6 months after the final licensed performance or activity
Other licensing applications and supporting records	Normally 3 years after production, unless longer retention is justified
Chaperone administration and allocation records	Normally 3 years after production, subject to safeguarding requirements
Production medical and emergency information	Review after production; normally remove within 3 months unless needed for another justified purpose
Workshop and summer school registration records	Normally 3 years after the activity
Routine workshop attendance records	Normally 3 years after the activity

Any record relating to safeguarding, injury, legal proceedings or financial transactions must follow the relevant longer retention period.

Photographs, Videos and Audio Recordings

Record	Retention Period
Photograph and video consent records	Retain while relevant material is being processed and for an appropriate period afterwards to evidence permissions
Identifiable promotional photographs	Review annually and remove when no longer required or appropriately authorised
Promotional video recordings	Review annually against purpose, permissions and continued necessity
Internal rehearsal recordings	Normally delete within 12 months of the relevant production or activity, unless continued retention is justified
Production films	Retain while there is a lawful, documented purpose, subject to consent arrangements, contracts and licensing conditions
External photographer or videographer files	Retention and deletion arrangements to be specified in the relevant agreement

Where consent is withdrawn, Performers will assess and act upon the request in accordance with applicable data protection law.

No photograph or recording will be retained indefinitely merely because it may be useful in the future.

Data Protection and Administrative Records

Record	Retention Period
Subject Access Requests and responses	Normally 3 years after completion
Personal data breach records	Normally 3 years after closure, longer where serious or ongoing
General enquiries	Normally 12 months after resolution
Routine administrative correspondence	Normally 3 years, unless a shorter or longer period is justified
Formal complaints	Normally 6 years after resolution, subject to the nature of the complaint
Superseded policies and governance documents	Normally 6 years after replacement, longer where relevant to legal or safeguarding matters
Supplier contact information	During the business relationship and reviewed after termination

Review and Secure Disposal

The Principal is responsible for overseeing the annual review of retained information.

Reviews will consider:

1. Whether the original purpose for retaining the information remains valid.
2. Whether a legal, safeguarding or contractual requirement requires continued retention.
3. Whether the information remains accurate and necessary.
4. Whether the record can be securely deleted, destroyed or anonymised.
5. Whether access permissions remain appropriate.

Electronic Records

Electronic information must be securely deleted from relevant systems, including ClassManager, Google Drive and other authorised storage locations, subject to system capabilities and applicable backup retention arrangements.

Removing a student from an active register does not necessarily mean all associated information has been deleted.

Paper Records

Paper documents must be securely shredded or destroyed when their retention period expires.

Confidential records must not be placed in general waste or recycling.

Extended Retention

Where a record is required for an ongoing safeguarding matter, complaint, investigation, legal claim or statutory requirement, its scheduled disposal must be suspended.

The reason for extended retention must be documented, and the record reviewed when the relevant matter concludes.

Responsibility and Oversight

Principal - Sam Gibbs
Responsible for implementing this schedule, reviewing retention arrangements, authorising disposal and ensuring appropriate records are maintained.

Designated Safeguarding Lead - Sam Gibbs
Responsible for reviewing the retention and disposal of safeguarding records.

Deputy Designated Safeguarding Lead - Jess Eaton
Supports appropriate safeguarding record management where authorised.

Authorised Administrative Staff
Responsible for maintaining accurate records and following the approved retention and disposal arrangements.

All staff must report any concerns about inappropriate retention, loss or unauthorised disclosure of personal information.

Annual Review

This schedule will be reviewed annually alongside the GDPR and Data Protection Policy.

Retention periods will also be reconsidered where legislation, safeguarding guidance, organisational activities or relevant contractual obligations change.