# Sylvia Young Theatre School

**Data Protection Policy**

| | |
|---|---|
| **Policy responsibility:** | **Maggie Melville** |
| **Updated or reviewed:** | **23rd July 2025**<br>**1st May 2025 Sean Wightman** |
| **ISI Reference:** | |

The directors recognise overall responsibility for ensuring that the Sylvia Young Theatre School complies with its legal obligations.

The Sylvia Young Theatre School has a Data Protection Licence Number **Z9762052**.

Data protection laws are overseen by the Information Commissioner who has powers to take legal action against businesses or individuals acting unlawfully. Any employee may make themselves individually liable to legal action by the Information Commissioner and/or by any individual whose information they have disclosed in breach of data protection legislation and who suffers loss as a result.

There have also been very high profile cases involving loss of data in breach of the legislation giving rise to very real damage to the reputation of the organisations concerned.

This policy is designed to prevent such potential damage to the Sylvia Young Theatre School, its employees, its students, its clients and to ensure that personal data processed by the company is dealt with in full compliance with the law.

The purpose of this policy is to ensure that the Sylvia Young Theatre School complies fully with its legal obligations in relation to the protection of personal information that it holds about or concerning any individual. All employees and directors must familiarise themselves fully with its contents and ensure that its terms are applied fully in relation to the handling or "processing" of personal information.

Those employees whose job involves the handling of personal information will receive appropriate training as required during their employment and the procedures for obtaining, retaining, updating, using, transporting, sending and destroying personal information. All of these functions are strictly confidential and any employee handling personal information in breach of the Sylvia Young Theatre School's data protection policy may face disciplinary charges that may, in serious cases, result in dismissal.

All staff read this policy and sign the SYTS Confidentiality Agreement as part of their induction. Further training takes place as part of the day-to-day practices required by their position.

This policy concerns personal information, especially sensitive personal information, held by the Sylvia Young Theatre School in relation to any person, whether they are, were or are about to become students, employees, clients, volunteers, service users and funders or any customer, supplier or contact. Personal data may include any information about any individual, held by the company.

The law contains some important concepts that define the obligations of the company and its employees. Although most employees are not expected to remember detailed legal definitions, a general understanding of the concepts is required to avoid inadvertent breaches and to ensure that employees can take further advice in relation to any particular situation that may give rise to concern.

The Sylvia Young Theatre School will nominate an individual responsible for data processing and compliance with data protection legislation.

**The Chief Privacy Officer (CPO) has the following responsibilities:**

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal information
- Approving contracts with Data Processors.

**Any questions or concerns relating to the company's or any individual employee's responsibilities should be referred to the employee's line manager.**
**The legislation:**

- Requires organisations to register if they keep records
- Governs the processing of personal information including 'personal sensitive data'
- Requires organisations to comply with eight principles
- Allows employees, clients and parents of students to request to see the personal information held on them.

**Data means recorded, stored information irrespective of the medium by which it is recorded or on which it is stored.**

**The Sylvia Young Theatre School will:**

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff and volunteers who handle personal information, so that they can act confidently and consistently
- Avoid causing harm to individuals by keeping information securely in the right hands
- Hold good quality information
- Give individuals as much choice as is possible and reasonable over what data is held and how it is used.

**The Sylvia Young Theatre School has identified the following potential key risks, which this policy is designed to address:**

- Breach of confidentiality (information being given out inappropriately)
- Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access
- Failure to establish efficient systems of managing changes leading to personal data being not up to date
- Harm to individuals if personal information is not up to date
- Failure to offer choices about the use of contact details.

**Examples are:**

- Staff with access to personal information could misuse it
- Staff or volunteers could continue to be sent information after they have stopped working for the Sylvia Young Theatre School if their records are not updated promptly
- Poor website security might give a means of access to information about individuals once individual details are made accessible online
- Staff may be tricked into giving away information, either about students, clients or colleagues, especially over the phone, for example by being persuaded to give a telephone number or address.

The ICT technicians are responsible for electronic security, and the Managing Director is responsible for approving Data-Protection-related statements on publicity materials, letters, etc.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal information they may handle in the course of their work.

Significant breaches of this policy will be handled under the Sylvia Young Theatre School's disciplinary procedures.

The Act aims to ensure that the legitimate concerns of individuals about the ways in which their personal information may be used are taken into account. In addition to being open and transparent, the Sylvia Young Theatre School will seek to give individuals as much choice as is possible and reasonable over what personal information is held and how it is used.

**Confidentiality applies to a much wider range of information than Data Protection**

- Data Protection only applies to information about individuals
- Data Protection only applies to Information which is recorded, either on paper in a sufficiently structured way as to be defined as a 'relevant filing system' or electronically.

**<u>The electronic systems used by the Sylvia Young Theatre School are:</u>**

Last updated 01 May 2025 by Sean Wightman

- Classroom.cloud - Student safeguarding software + remote desktop for teachers to monitor student activity.
- MyConcern - safeguarding software for staff to report student issues
- Microsoft Sharepoint - backup software
- Doublefirst Engage - for Full Time School students and their parents; Full and Part-Time staff, volunteers and catering contractors
- Microsoft Remote Desktop - used for accessing the Engage system remotely

- AgentFile - Historic Filemaker Pro database used by the SYTS Agency for client details
- TagMin - Web based Theatrical Agency software used by the SYTS Agency
- Active Network: Camp and Class Manager - Online booking system. Full Time School Scholarship Applications; Part Time School students; Holiday Course students; Full Time School Acrobatics students; Management of SYTS Part Time finances and credit card payments
- Stripe - online payment software
- PayPal - online payment software
- Formsite - Information relating to - Employment; Application Forms; Waiting Lists; Uniforms; Staff Updates; Staff Reviews; Training Logs; Studio Hire T&C's
- Google/G-Suite for Education/Google Workspace - Google Drive for the SCR; Staff Holiday Planning; Student Personal Information, including Sensitive Information; Staff Personal Information, including Sensitive Information; Student and Parent Consent Forms; Student Performance Licences; Data Collection; Student Medical Information and 'Care and Concern' Updates
- Matrep - School Reporting software for termly school reports (Interim, full and Assessments). Also contains student photographs. System is accessed by Staff for administration, Teachers (for submitting reports) and parents (for viewing reports)
- NetSupport DNA - for eSafety and safeguarding. Netsupport gives us keyword and phrase monitoring to alert us of any online activity that may place a student at risk when using school devices; internet monitoring of websites visited. Netsupport also has the option for students to report concerns directly to trusted members of staff (our safeguarding leads) – and much more.
- Academic Teaching Apps
- Google Classroom
- Adobe Creative Cloud - Adobe Premiere (video editing software), Adobe Photoshop (photo editing software), Adobe Indesign (dtp software), Adobe Illustrator (design software)
- EventBrite - for School Concert and Presentation Ticket booking
- Dropbox
- Freshdesk: For the IT department - Logging and Information Technology Issues
- Peninsula - Staff HR Management
- MyConcern - safeguarding referral, recording and storage system
- Synology - local backup system and file sharing.
- HikVision - CCTV software and CCTV system
- Apple OSX Server - IT directory system for the IT suites
- AirParrot - Software for Windows machines to wirelessly project to our school Apple TV devices

- Zerotier - Zerotier is a client application that enables devices such as PCs, phones, servers and embedded devices to securely connect to our own peer-to-peer secure virtual network. The IT team use this for technical support
- Tailscale - is another client application that enables devices such as PCs, phones, servers and embedded devices to securely connect to our own peer-to-peer secure virtual network. The IT team use this for technical support
- Splashtop - Remote Access software for technical support both in and out of the building
- Microsoft Office Suite - Word, Excel, Outlook and Powerpoint
- Apple Remote Desktop - High end remote access software used in conjunctions with both Zerotier and Splashtop
- Avast Premium - Antivirus software to protect the computers
- Malwarebytes - Anti Malware software to protect the computers
- Parallels Desktop - Software in order to run Windows software on a Mac
- JAMF Pro (formerly Casper Suite) - MDM (mobile device management) software for managing the IT suites / deploying software / locking down computers
- CloudReady - software to transform old equipment into capable Google Chrome devices.
- Backblaze - Online Backup

Electronic systems are password protected.

Staff are instructed to have a clear desk policy and to lock away sensitive information.

A Business Continuity Plan is in place which ensures the regular backup of all electronically stored data.

Paper records are kept for:

- current Full Time School students in lockable filing cabinets in a locked room;
- past students in our locked archive;
- current staff in the vocational office and the accountant's office;
- past staff in our locked archive.

Access to these records is defined on a "need to know" basis; no one has access to information unless it is relevant to their work.

Confidentiality has its limits. There will always be cases where it may be appropriate to break confidentiality. Such situations must be judged on a case by case basis but as a guiding principle, where the health and safety of an individual is called into question then this may be the right option.

For example in work with teenagers, discussing how much information will be shared with their parents or carers needs to be dealt with sensitively and safely.

The Sylvia Young Theatre School is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed;
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

**Data Subjects will generally be informed in the following ways:**

- the handbook for staff/parents and carers
- the welcome pack for students/clients
- in the letter of appointment and welcome pack for staff, with occasional reminders in the newsletter
- during the initial interview with clients.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

The Sylvia Young Theatre School has a privacy statement for Data Subjects, setting out how their information will be used. See website. (See Appendix A.)

Staff, volunteers and directors will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Appendix B).

Where anyone within the Sylvia Young Theatre School feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of the Chief Privacy Officer. All such disclosures will be documented.

The Sylvia Young Theatre School will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed with privacy in mind and to facilitate accurate data entry of individuals information
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request the Data Controller must provide a permanent, intelligible copy of all the personal information about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of personal information (or may choose to provide more), and certain information may be withheld. This includes some third party material, especially if any duty of confidentiality is owed to the third party and limited amounts of other material. (“Third Party” means either that the information is about someone else, or someone else is the source.)

Any subject access requests will be handled by the Chief Privacy Officer. Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Chief Privacy Officer without delay.

All those making a subject access request will be asked to identify who may also hold information about them, so that this information can be retrieved. Where the individual making a subject access request is not personally known to the Chief Privacy Officer their identity will be verified before handing over any information. Such requests must be handled within the legal time limit of 30 days. Requests are infrequent and can be complex. They may require taking legal advice.
The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

**Right to Retention**

We will make considered decisions regarding retention of information in line with guidance from our insurers, best practice in terms of educational needs and any other requirements that are both justified and legitimate.

**Right to Erasure**

The Data Subject may request this right. There is a 30 day time period to accede to this right. There may be exemptions for example if there is a safeguarding concern, if it involves permission from a third party. The Data Controller will ensure that the Data Subject is kept informed of the progress made in response to a request for erasure.

Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

This policy provides guidance on basic compliance and offers examples of good practice. However further essential information enabling staff to familiarise themselves with provisions and codes of practice relating to data protection can be accessed on the Information Commissioner's website

Please click the link for our Examinations Policy

Click here

*For the website, additional information is usually included. This would cover:*

- *Collection of IP addresses, and whether it links them to the individual in order to track their future visits*
- *Cookies and what are they used for.*

**Notes to go with medical information on school trips**

Data Protection and Personal Sensitive Information

First aid equipment and medical information are stored in a rucksack with a padlock

When the first aid equipment and personal sensitive information is in use - any time during the trip - there is no need to lock it away. In fact it shouldn't be locked away in case there's an emergency and it's needed.

After the trip is over and the students have gone home, the teacher should lock the rucksack using the padlock provided and store the rucksack safely before returning it to school.

For a trip involving a smaller group of students the teacher can keep the personal sensitive information in their own bag and destroy it when the visit is over. A copy of all paperwork is left with the school office so if there was follow up afterwards there would be proof of what the teacher had had with them.

**GDPR Register**

The School keeps a GDPR Register.
There is a termly check with key departments to ensure that there have been no breaches in any area and to update the list of electronic systems.
In the case of a breach, the details are carefully examined, a decision is made as to whether it is a low, medium or high risk breach and whether the ICO should be informed. The member of staff responsible for the breach is interviewed and is then contacted in writing with any decision regarding the breach. A record is kept in the GDPR register. Further training is put in place where necessary.

**Update July 2023 following recent GDPR training**

- There are new laws governing what the police can ask for. The School can say no and wait for a court order.
- Always inform the ICO if there's a complaint
- If the School receives a SARS request, ask for ID if there is uncertainty about who is requesting the information.
- If the request is from a third party make sure the School has permission from the owner.
- 12 years old is considered to be the age for a child to own their data. But case by case consideration is advised as the age is not an absolute. The School should be satisfied the child is able to make decisions for themselves.
- A SARS request is not a green light to disclose everything. Eg parent/carer/child
- The time limit is paused while the school is awaiting clarification.
- The data released has to be useful and reasonable.
- Exemptions include - references given in confidence.
- In the case of a vexatious request the school may charge a fee.

**Staff Training**

**GDPR Refresher - 09/2025**

Email Etiquette Guide

Staff training about hacking and about how to spot phishing emails, as these are becoming more  sophisticated, is planned.

**Appendix A and Appendix B**

Click here

Appendix A - Privacy Notice
Appendix B - To sign that you have read and understood our ‘Data Protection Policy’ and agree to its terms.