

## GDPR Privacy Statement

We are Big Little Theatre School Ltd. and we confirm that we will comply with the provisions of the General Data Protection Regulation (GDPR) when processing personal data about you. The General Data Protection Regulation will have superseded the Data Protection Act 1998 (DPA) on the 25<sup>th</sup> May 2018.

For the purposes of the law and these principles, a 'data controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In relation to the majority of our data, we are data controllers but can also be a data processor. A data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

We will where it is necessary to properly carry out our business collect confidential or sensitive personal data (for example where it is necessary to obtain DBS checks, or in relation to our confidential health, welfare or safeguarding information). In relation to this we will:

- only process the personal data provided in accordance with the data controller's instructions and in accordance with our contract with them
- implement technical and organisational measures in line with the GDPR to ensure the fair and lawful processing and the security of such data
- not disclose the data or transfer it to any third party without the explicit permission of the data controller, unless we are legally obliged to do or it is permitted and authorised by the contract with the data controller
- ensure that appropriate records are kept in order that we are able to demonstrate compliance with GDPR principles
- comply with our obligations to notify the regulatory authorities of any data breach.

The person responsible for GDPR compliance for Big Little Theatre School Ltd. is Colin Billing..

We shall use appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. We shall not sub-contract any processing of personal data unless the sub-contractor has agreed that the personal data continues to be subject to an appropriate level of protection. To the extent we act as data processor for you, we shall only process personal data in accordance with your instructions.

We shall answer your reasonable enquiries to enable you to monitor compliance with this clause.

### Personal data we collect and process

The type of personal data that we process depending on the type of services we are engaged with you can be;

Names  
Addresses  
Mob / Tel Nos.  
Email Addresses

Relevant educational & medical information  
Official forms of identification (driving license, NI numbers etc.)  
Examination & audition results

The categories of the data subjects depending on what services we are engaged with you can be;

Individuals which can be parents, legal guardians and children.

## How we use personal data

In order to carry out services of the agreed engagement between us and for related purposes such as updating and enhancing our customer records, analysis for management purposes, legal and regulatory compliance and crime prevention we may obtain, process, use and disclose personal data about you. You shall ensure that any disclosure of personal data to us complies with the GDPR.

Our policy is to collect only the personal data necessary for agreed purposes and we ask customers to only share personal data where it is strictly needed for those purposes. We collect personal data from our customers or from third parties acting on the instructions of the relevant customer.

We process personal data to enable us to provide services such as enrolment in classes, courses and activities, examinations, events & productions as part of the range of services we offer. We also process personal data in the administration and management of our business.

We will only share personal data with others when we are legally permitted to do so. When we share data with others, we put contractual arrangements and security mechanisms in place to protect your data. We use third parties located in other countries to help us run our business which are SaaS providers. As a result, personal data may be transferred outside the countries where we and our customers are located. This includes countries outside the European Union ("EU"). We ensure that all third party SaaS providers comply with the appropriate safeguards and EU data export restrictions when personal data is exported outside of the EU.

Your contact details are used to provide you with information about our services and other information which we think will be of interest to you or your business, unless you tell us not to.

We will never disclose any of your personal data to a third party unless we have obtained your specific permission to do so (for example to an Examination Board for the purpose of examination entry)

## How we collect and store personal data

We can collect your personal data in a variety of different ways. These can be via email communication, website contact form, hard copy of letters and telephone calls.

We take the security of your data we hold seriously. We have a policy including procedures and training in place covering data protection, confidentiality and security and regularly review the appropriateness of the measures we have in place to keep the data we hold secure.

We use SaaS systems to store and process your personal data so that we can carry out the services of the agreed engagement. The SaaS systems that we use have the data stored

securely by using industry-standard encryption which is the same technology that banks use to protect data.

Personal data may be transferred outside the countries where we and our customers are located. This includes countries outside the European Union ("EU"). We ensure that all third-party SaaS providers comply with the appropriate safeguards and EU data export restrictions when personal data is exported outside of the EU.

At Big Little Theatre School we take privacy and security very seriously. We have taken steps with our internal processes and procedures to ensure that your personal data is safe-guarded and secure.

We do not store login credentials that have access to your personal data un-securely i.e using excel spreadsheets or on hard copies of paper. All login credentials are stored using an industry-standard encrypted password manager. This password manager is controlled by us and we can disable user accounts should we have to.

All of the computers at Big Little Theatre School are regularly scanned for malware, viruses and spyware and security updates are regularly applied to all of the computers that we have in the office as soon as they become available.

## How long do we retain your personal data

We are subject to legal and professional obligations. We need to keep certain records to demonstrate that our services are provided in compliance with those obligations and those records may contain personal data.

Personal data processed is kept by us for as long as is considered necessary for the purpose for which it was collected (including as required by applicable law). In the absence of specific legal, regulatory or contractual requirements, our retention policy period for records and other documentary evidence created in the provision of services is 7 years.

## How to access & control your personal data

You have the right to access your personal data and obtain confirmation that your data is being processed.

A copy of this information will be provided free of charge. If a request becomes manifestly unfounded, excessive or particularly repetitive then a fee will be charged. The fee will be based on the administrative cost for providing this information.

Information will be provided to you without delay and at the latest within one month of receipt. We will be able to extend the period of compliance by a further two months where requests are complex or numerous. In this case, you will be informed within one month of the receipt of the request and be given an explanation for the extension.

If a request becomes manifestly unfounded, excessive or particularly repetitive we do have the right to refuse to respond to this request. You will be informed with an explanation as to why your request was refused and you have the right to complain to the supervisory authority and to a judicial remedy.

We must verify the identity of the person making the request using "reasonable means". We will provide information for your request electronically in a commonly used format if your request is made electronically.

You are entitled to have personal data rectified if it is inaccurate or incomplete. We will respond to this request within one month. This can be extended by two months where the request for rectification is complex.

You have the right to have your personal data erased unless there is a compelling reason for it to not be deleted. You have the right for your personal data to be erased in the circumstances below;

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data must be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

We can refuse to comply with your request for erasure in the circumstances below;

- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- the exercise or defence of legal claims.

You have the right to request that your personal data is no longer processed. You have the right to data portability. This will be provided by us free of charge and will be in a commonly used electronic format such as a CSV file.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You have the right to object to profiling or automated decision making. We do not carry out any profiling or automated decision making.

You can easily ask to withdraw consent as it was to give it in the first place. When we update our privacy policy we will inform our existing customers.

If you do want to complain about our use of your personal data, please contact us below with the details of your complaint. You also have the right to register a complaint with the Information Commissioner's Office ("ICO"). For further information on your rights and how to complain to the ICO, please refer to their website.

To request access to personal data that we hold about you, or request that we update or correct any personal information we hold about you or want to complain about the use of your personal data then please do so in writing by emailing [info@biglittle.biz](mailto:info@biglittle.biz)

## Data breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We will do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.

We have breach detection and investigation procedures in place. This will facilitate decision-making about whether or not we would need to notify the relevant supervisory authority and the affected individuals. We will also keep a record of any personal data breaches, regardless of whether we are required to notify the relevant supervisory authority.

## Confidentiality

Communication between us is confidential and we shall take all reasonable steps to keep confidential your information except where we are required to disclose it by law, by regulatory bodies, by our insurers or as part of an external peer review. Unless we are authorised by you to disclose information on your behalf this undertaking will apply during and after this engagement.

We may, on occasions, subcontract work on your affairs to other subcontractor professionals. The subcontractors will be bound by our customer confidentiality terms.

We reserve the right, for the purpose of promotional activity, training or for other business purpose, to mention that you are a customer. As stated above we will not disclose any confidential information.

## Controller and processor terms

### Duration of processing

We will process personal data in order to carry out services of the agreed engagement until we are instructed to stop.

### Type of personal data and categories of data subject

The type of personal data that we process depending on the type of services we are engaged with you can be;

Names

Addresses

Mob / Tel Nos.

Email Addresses

Relevant educational & medical information

Official forms of identification (driving license, NI numbers etc.)

Examination & audition results

The categories of the data subjects depending on what services we are engaged with you can be;

Individuals which can be parents, legal guardians and children.

## The obligations and rights of the data controller

### Compulsory terms

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

## Children

We have consent (as a lawful basis) from a child's parent or legal guardian to be able to process a child's personal data for us to carry out our agreed services. In the UK only children aged 13 or over are able provide their own consent.

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.