

## Data Protection and Retention

*This policy reflects First Act Arts (and all its associated parties) commitment to the General Data Protection Regulation (GDPR) and the provision of the 2018 Data Protection Act. This policy covers the processing of personal data wholly or partly by automated means and the processing (other than by automated means) of personal data which form part of a filing system or are intended to form part of a filing system. We take GDPR extremely seriously and hope to reflect, in this policy, the measures we take to go above and beyond our duty to protect the data of our families and tutors.*

### **Our Responsibility**

Christopher Phillips acts as the Data Protection Officer for First Act Arts. Through this role, our DPO will keep up to date with regulation and legislation through regular CPD training (which will be disseminated down to tutors). This CPD will include regular updates in the collection, processing, storage, and destruction of data.

We guarantee that all the data principals (outlined below) are adhered to and the rights of all data subjects are respected. Any data risks are assessed, and any new processing activity introduced is subject to strict analysis and review.

Regular internal and independent reviews of processing activity and processing documentation will be carried out and organisational and technical measures will be reviewed and implemented. Any data breaches impacting on the rights and freedoms of data subjects will be reported to the ICO.

### **Data Principles**

First Act is committed to the principles relating to processing of personal data, in that personal data will be processed lawfully, fairly and in a transparent manner in relation to the data subject. It will only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. It will also be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

First Act will do as much as possible to support parents in ensuring that the data is accurate and, where necessary, kept up to date. All data should be kept in a form which permits identification of data subjects for no longer than is necessary. It should be processed in a manner that ensures appropriate security of the personal data.

### **Lawful Processing**

We will only process personal data where a lawful basis for processing exists. Specifically, where consent to the processing of his or her personal data for one or more specific purposes has been given; processing is necessary for the performance of a contract to which a data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another

natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

## Registration

Upon joining First Act Arts, parents must provide core details required for membership. These can be done independently at home, or at the studio face-to-face with a member of the SLT.

We collect:

- Student and Guardian Name
- Guardian Email
- Guardian Phone Number
- Details Of Medical Conditions or Additional Notes

## Reviewal of Personal Data Meetings

As part of our ongoing GDPR practice, our DPO will conduct termly Personal Data Reviews with parents via email. This process will check that all the information we hold is correct and up-to-date.

## Photo and Video Media

Parents can opt out of photo or video media being taken of their child. Materials will be used for marketing and promotional purposes, which includes social media, production promotional videos, First Act promotional videos, posters, leaflets, website, and external publishing (e.g. newspapers, magazines, brochures etc.).

Parents and carers must understand that if permission is granted and media is posted on the agreed channels, that should permission be revoked, First Act will do so to the best of its ability; however, materials which may have been used according to this policy for external or physical publishing will not be able to be controlled.

Should a student leave First Act, unless a data removal request is made for all media data, any photo or video media collected may still be used for the agreed purpose above.

## Audition and Assessment Data

In some situations, parents may share data or media of students for assessment and audition purposes. This is acceptable in situations where normal face-to-face assessment or auditions can not be held. Prior to the submission of this data or media, parents should be made aware that:

- If data is shared via email, once data or media has been used for its desired purpose, it will be destroyed;
- If data is shared via social media accounts (e.g. Facebook Messenger), once data or media has been used for its desired purpose, the conversation or messenger chat containing the media will be deleted permanently via the First Act official account.

## Gmail and GDrive

As of the time of this policy, First Act stores data within the First Act secured GDrive and Gmail Business Account. This is accessible only by SLT members. Access to this GDrive and the Gmail account can be made via a Subject Access Request. There should be no other sources of First Act data, with the exception of promotional, marketing, and social media.

## The Rights of Students, Parents and Tutors

First Act supports the rights of data subjects (or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to fair and transparent processing
- Right of access
- Right of rectification
- Right to erasure (the right to be forgotten)
- Right to restrict processing
- Right to be notified of erasure, rectification or restriction
- Right of data portability
- Right to object to processing
- Right to object to processing for the purposes of direct marketing
- Right to object to processing for scientific, historical or statistical purposes
- Right to not be evaluated on the basis of automated processing
- Right to withdraw consent at any time
- Right to be notified about a data breach
- Right to an effective judicial remedy against a supervisory authority
- Right to lodge a complaint with supervisory authority
- Right to an effective judicial remedy against a controller or processor
- Right to compensation.

## Erasure and Data Destroying

In situations where a data subject has requested data erasure (or data has fallen out of line with this policy) all data held on for the data subject will be removed. Any electronic data will be permanently deleted and any paper-based data will be destroyed. Data subjects have the right to a full breakdown of all data destroyed and the means in which it has been done.

## Data for Marketing and Data Sharing

First Act uses data collected for marketing in two different ways. Firstly, marketing materials may be produced, given the right permissions have been granted, and distributed. Secondly, we used data collected to market internally

regarding classes, events and productions hosted by First Act Arts. Social Media accounts may be used to market events which are not hosted by First Act but may be of interest.

First Act does not share or sell data to any third parties. Where data is shared with third-party processors, they will only process data with the explicit instructions (either contractual or through a data sharing agreement) of First Act and shall not hold or process the data for any other purpose. The minimum data required for the processing task will be provided for the processing. Any third-party processors, where contracts or data sharing agreements are required for the processing to take place will be required to provide evidence of their commitment to GDPR compliance.

Where we have a legal obligation to share information with law enforcement, agencies and government bodies for legitimate purposes relating to criminal justice and taxation we will do so. We will share information if there is an issue that jeopardises the safety or security of staff, students of school visitors.

## Information Commissioner's Office

For the purposes of data protection, First Act Arts is a data controller, responsible for the determination of the purposes and means of the processing of personal data and where the purposes and means of such processing takes place. As such, First Act is supervised by the Information Commissioner's Officer and will pay the data protection fee required by law.

The Data Protection Officer will be the principal point of contact with the Information Commissioner's Office.

## Data Breaches

In the case of a personal data breach, First Act Arts shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

In order to evaluate the personal data breach, First Act shall inform and involve the Data Protection Officer in the assessment of the breach and in the execution of the data breach procedure to contain and manage the breach.

A notification shall at least:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
- Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.
- Describe the likely consequences of the personal data breach.
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

- Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

First Act Arts shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a data breach log. The log shall enable the Information Commissioner's Officer to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in the identification of new data handling processes and training requirements.

## Examples of Data Breaches

Data breaches could include, but are not limited to:

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. a laptop, mobile phone, tablet device or memory stick.
- A letter or email containing personal and/or confidential data sent to the wrong address (including internal staff or third parties) or an email to an unauthorised group of email boxes.
- Personal data disclosed orally in error in a meeting or over the phone – including “blogging” where information is obtained by deceiving First Act, or where information has been disclosed without confirming the true identity of the requester.
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible.
- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions.
- Sensitive information left on a photocopier or on a desk in unsupervised premises.
- Unauthorised alteration or deletion of information.
- Not storing personal and confidential information securely.
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures.
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.
- Unauthorised access to IT systems because of misconfigured and/or inappropriate access controls.
- Hacking or phishing attacks and related suspicious activity.
- Virus or malware attacks and related suspicious activity.
- ICT infrastructure-generated suspicious activity.
- Divulging a password to another user without authority.

## Subject Access Request

First Act Arts is committed to ensuring that individuals' rights to their own personal information can be appropriately exercised by providing adequate training for staff to recognise and handle subject access requests and ensuring that everyone handling personal information knows where to find further guidance on individuals' rights in relation to

their own personal information. It is vital that queries about individuals' rights to their own personal information are dealt with effectively and promptly and that First Act are fair and transparent in dealing with a subject access request.

All subject access requests need to be logged to assist the Information Commissioner's Office with any complaints related to subject access as well as identifying any issues that may assist in the identification of new data handling processes and training requirements. The DPO and SLT are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the GDPR and in compliance with this policy. All staff have a responsibility to recognise a request for information and ensure it is passed to the Data Protection Officer within two working days.

## DBS and Chaperoning License Evidence Collection

In order to remain in line with our 'Safeguarding Policy', tutors at First Act Arts require Enhanced DBS checks and chaperones require a Warrington Borough Council Chaperones License.

There are data collection requirements for both of these processes. Throughout these applications, the guidelines set out in the rest of this policy will apply, and data held will be stored electronically within the secure GDrive. Following the completion of the application, the data received will be deleted and replaced with the DBS and Chaperone license evidence.

## Passwords

All passwords used for First Act Arts accounts and devices must be in line with the following principles:

- They are change on a regular basis
- All passwords must use a combination of upper and lower case and plus at least one not standard char (!\$& etc) which makes them a lot harder to hack
- All users will have different logins, ie no shared logins

If any member of the SLT team leaves, all accounts that they possess relating to First Act must be terminated and any password combinations that they know of (e.g. door locks) must be changed with a period of 24 hours.

## Expired Data Checks

Prior to any expired data being destroyed, checks should be carried out by the DPO and SLT regarding the suitability of the data destruction.

These checks will include looking at whether the documents been checked to ensure they are appropriate for destruction: is retention required to fulfil statutory obligations or other regulatory obligations, including child protection, is retention required for evidence, is retention required to meet the operational needs of the service, is retention required because the document or record is of historic interest, intrinsic value or required for organisational memory?

In situations where data is not destroyed due to these checks, all parties involved in the creation of this data, including the original data subject, whether or not they are still present at First Act, should be involved in granting permission for its renewal.

## Student and Parent Information

Data which contains information regarding student or parent information will be stored on First Act's secure GDrive.

It will be stored while the student remains a member of First Act Arts and will be destroyed following the termination of their membership, with the exceptions of notes on behaviour, accident and safeguarding; photographs and video media; and payment history.

## Behaviour, Accident and Safeguarding Logs

Data stored as part of our 'Safeguarding Policy' and our 'Health and Safety Policy' will be securely stored on First Act's GDrive. They will be stored for a period of no longer than 5 years unless they are being used as part of an ongoing investigation or claim.