Bristol One Act Drama Festival – Data Protection Policy

Context and overview

Policy prepared by: Brian Fisher

Approved by Committee: 24/05/2018

Next review date: 24/05/2019

Introduction

The Bristol One Act Drama Festival Committee (hereinafter referred to as 'the Committee') runs The Bristol One Act Drama Festival, a preliminary round of the All England Theatre Festival (AETF) and needs to gather and use certain information about individuals.

The individuals can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organisation's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures the Committee:

- Complies with data protection law and follows good practice
- Protects the rights of customers, Committee members, volunteers, patrons and Sponsors
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulation ("GDPR") comes into force on the 25th May 2018, superseding the Data Protection Act 1998.

Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the GDPR, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by six important principles, summarised below:

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimisation

4. Accuracy

5. Storage limitation

6. Integrity and confidentiality

As a data controller, the Committee shall be responsible for, and be able to demonstrate compliance with these principles.

People, risks and responsibilities

Policy scope

This policy applies to:

- The Committee members
- All staff and volunteers in connection with the Bristol One Act Drama Festival
- All contractors, suppliers, sponsors and other people working on behalf of the Bristol One Act Drama Festival and all subsequent rounds of the AETF and other associated drama festivals for which the Committee is responsible

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks

This policy helps to protect the Committee from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately or via poor security.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the organisation could suffer if hackers successfully gained access to sensitive data.
- Individuals being harmed through data being inaccurate or insufficient

Responsibilities

Every member of the Committee has some responsibility for ensuring data is collected, stored and handled appropriately in line with this policy and data protection principles.

The appointed data protection officer is responsible for:

- Keeping the Committee updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from everyone covered by this policy
- Dealing with requests from individuals to see the data the Committee holds about them (also called 'subject access requests')
- Checking and approving any contracts or agreements with third parties that may handle personal data
- Notification to the Information Commissioner's Office as required
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services the Committee is considering using to store or process data. For instance, cloud computing services
- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets
- Ensuring marketing initiatives abide by data protection principles

The only people able to access data covered by this policy should be those who need it for appropriate reasons as approved by the Committee. Data should not be shared informally. Committee members should keep all data secure, by taking sensible precautions and following the guidelines below:

- Strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the Committee or externally
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of

Data storage

These rules describe how and where data should be safely stored. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason. When not required, the paper or files should be kept in a locked drawer or filing cabinet. Committee members should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between Committee members
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services
- Servers containing personal data should be sited in a secure location
- Data should be backed up frequently and tested regularly
- All servers and computers containing data should be protected by approved security software and a firewall if appropriate

Personal data shall be retained for appropriate periods of time balancing legal obligations, with operational, heritage and privacy considerations.

Data use

Personal data is of no value to the Committee unless they can make use of it. When working with personal data, Committee members should ensure the screens of their computers are always locked when left unattended. Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure. Data must be encrypted or password protected before being transferred electronically. Personal data should never be transferred outside of the European Economic Area.

Data accuracy

The law requires the Committee to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all Committee members who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. Data will be held in as few places as necessary. Committee members should not create any unnecessary additional data sets. They should take every opportunity to ensure data is updated.

The Committee will make it easy for data subjects to update the information held. Any inaccuracies should be updated as soon as they are discovered. For instance, if a contact

can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by the Committee will have the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data
- Other supplementary information, including:
    - The purposes of the processing
    - The categories of personal data concerned
    - The recipients or categories of recipient to whom the personal data has been or will be disclosed
    - Where possible, the envisaged period for which the personal data will be stored
    - The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
    - The right to lodge a complaint with a supervisory authority
    - Where the personal data is not collected from the data subject, any available information as to its source

If an individual contacts the Committee requesting this information, this is called a subject access request.

Subject access requests from individuals should be made in writing or by email to any member of the Committee. The Committee will provide the information free of charge in a commonly used electronic format.

However, the Committee can charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive. The Committee may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information. The relevant data will be provided within one month of receipt of that request, unless there are exceptions where requests are complex or numerous.

A Committee member will always verify the identity of anyone making a subject access request before handing over any information.

The Committee will also respond to other requests from data subjects, including the right of rectification and the right to erasure.

Providing information

The Committee aims to ensure that individuals are aware that their data is being processed, and that they understand:

• How the data is collected and being used

• How to exercise their rights

To these ends, the Committee has a privacy statement, setting out how data relating to individuals is used. These are available on request, with a summary available on the Bristol One Act Drama Festival website.

Please note: our website may provide links to other websites. Our privacy notice only applies to the Bristol One Act Drama Festival website, when individuals link to other websites they should read the privacy notices on those sites.

24.05.2018