Confidentiality of Information, Data Protection and Personal Data Policy

Introduction

Every Festival Angel who is involved with managing the volunteers lists and/or the collation of information and/or is dealing with Festival Goers (customers) debit/credit payments will receive, use and maybe store personal information about our volunteers or customers. It is important that if you are using this information, it is handled lawfully and appropriately in line with the requirements of the current Data Protection Act which have been superseded by the General Data Protection Regulation 2018 in May 2018 (collectively these laws are referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

You must observe absolute confidentiality concerning the affairs of the Festival Angels and not use any information other than as required to perform your volunteer duties. This includes all aspects of the organisation's business, as well as the firms and individuals that we work with.

You should seek further guidance if you are at all uncertain as to whether confidential information can be disclosed.

Disclosing confidential information without permission may be a criminal offence.

The duty to observe confidentiality is ongoing and does not cease after you leave Festival Angels.

About this policy

This policy, and any other documents referred to in it, sets out the basis on which the Organisation will process any personal data we collect or process.

This policy does may be amended at any time.

The Steering Group is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to Nic Sheppard, Chair of the Steering Group.

Festival Goers (Customer) Information and Volunteer Information

The collation of all customer and volunteer data, including credit card information is covered by Data Protection legislation and strictly governed by the FCA. (Financial Conduct Authority)

All volunteers are tasked with ensuring compliance of the following principles:

- Never leave any personal data pertaining to a customer on show or in a place where it can be seen by others
- Never take a photocopy or make an imprint of a customer's credit/debit card
- Only collect the data you need and then only keep it for as long as absolutely necessary.
- Paper documents that contain credit card data or bank details must be kept secure and then destroyed when they are no longer needed.
- If a customer sends personal information to you by email, for example, you should delete it as soon as it has been used in the correct manner.

What is personal data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in the Organisation's possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

Data Protection Principles
Anyone processing personal data, must ensure that data is:

- Processed fairly, lawfully and in a transparent manner
- Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose
- Adequate, relevant and limited to what is necessary for the intended purposes
- Accurate, and where necessary, kept up to date
- Kept in a form which permits identification for no longer than necessary for the intended purposes
- Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual

Fair and Lawful Processing
The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, the Organisation will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Processing for Limited Purposes
In the course of our business, the Organisation may collect and process the personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

Festival Angels will only process personal data for specific purposes or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Notifying Individuals
If we collect personal data directly from an individual, we will inform them about:

- The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing
- Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued
- The types of third parties, if any, with which we will share or disclose that personal data
- The fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place
- How individuals can limit our use and disclosure of their personal data

- Information about the period that their information will be stored or the criteria used to determine that period
- Their right to request from us as the Controller access to and rectification or erasure of personal data or restriction of processing
- Their right to object to processing and their right to data portability
- Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn
- The right to lodge a complaint with the Information Commissioners Office
- Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources
- Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within one month.

We will also inform data subjects whose personal data we process, that we are the data controller with regard to that data, what our contact details are and who the Data Protection Compliance Manager is.

Adequate, Relevant and Non-excessive Processing
We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accurate Data
We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely Processing
We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Processing in line with Data Subjects' Rights
We will process all personal data in line with data subjects' rights, in particular their right to:
- Confirmation as to whether or not personal data concerning the individual is being processed
- Request access to any data held about them by a data controller (see also Clause on Subject Access Requests)
- Request rectification, erasure or restriction on processing of their personal data
- Lodge a complaint with a supervisory authority
- Data portability
- Object to processing including for direct marketing
- Not be subject to automated decision making including profiling in certain circumstances

Data Security/Breach
We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if s/he agrees to comply with those procedures and policies, or if s/he puts in place adequate measures him/herself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the intranet or central computer system not individual PCs or laptops.

Security procedures include:

- Data minimisation
- Pseudonymisation and encryption of data
- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- Equipment. Volunteers must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Any data breach must be reported immediately to your Team leader or a Coordinator. The Organisation has a responsibility to ensure than any data breach that requires escalation is reported to the Information Commissioners Office (ICO) within 72 hours.

If a breach does not require escalation to the ICO it must still be reported and logged internally, in order to comply with the regulations.

Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of our group who are involved in the management of the Organisation.

Subject Access Requests

Individuals must make a formal request for information we hold about them. Volunteers who receive a request should forward it to the Steering Group immediately.

When receiving telephone enquiries, the Organisation will only disclose personal data held on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it
- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked

Where a request is made electronically, data will be provided electronically where possible.

Our volunteers will refer a request to their Team Leader or a Coordinator for assistance in difficult situations.

All requests must be responded to within one month.

Changes in personal circumstances

We need to keep accurate records of key information on all employees . It is essential that any such changes are provided without delay.

In order to comply with our statutory duties, we need to know of any changes in your personal circumstances, which affect or could potentially affect your work as a volunteer with the Organisation.