Fizzypig Ltd

Data Protection Policy and Procedures

1. Introduction

Fizzypig Ltd (hereafter FP) collects and uses information about people with whom it communicates. This personal information must be dealt with properly and securely however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 1998.

FP regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals. To this end FP fully endorses and adheres to the Principles of Data Protection, as set out in the Data Protection Act 1998.

2. Purpose

The purpose of this policy is to ensure that FP directors, volunteers, employees, members, self-employed contract workers and others representing FP (hereafter referred to as 'personnel') are clear about the purpose and principles of Data Protection and to ensure that it has guidelines and procedures in place which are consistently followed.

Failure to adhere to the Data Protection Act 1998 is unlawful and could result in legal action being taken against FP or its personnel.

3. Principles

The Data Protection Act 1998 regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Data users must comply with the data protection principles of good practice which underpin the Act. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this FP follows the eight Data Protection Principles outlined in the Data Protection Act 1998, which are summarised below:

I. Personal data will be processed fairly and lawfully
II. Data will only be collected and used for specified purposes
III. Data will be adequate, relevant and not excessive
IV. Data will be accurate and up to date
V. Data will not be held any longer than necessary
VI. Data subject's rights will be respected
VII. Data will be kept safe from unauthorised access, accidental loss or damage
VIII. Data will not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The principles apply to “personal data” which is information held on computer or in manual filing systems from which they are identifiable. FP personnel who process or use any personal information in the course of their duties will ensure that these principles are followed at all times.

4. Procedures

The following procedures have been developed in order to ensure that FP meets it’s responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by FP falls into 2 broad categories:

A. FP’s internal personnel data records
B. FP’s external data records; clients, partners, venue providers, and other contacts.

FP as a body is a DATA CONTROLLER under the Act, and the Executive Committee/Board is ultimately responsible for the policy’s implementation.

A. Internal data records

Purposes

FP obtains personal data (names, addresses, phone numbers, email addresses), application forms, and references and in some cases other documents from personnel. This data is stored and processed for the following purposes:
• Recruitment
• Equal Opportunities monitoring
• Volunteering opportunities
• To distribute relevant organisational material e.g. meeting papers
• Payroll

Access

The contact details of FP personnel will only made available to other FP personnel. Any other information supplied on application will be kept in a secure filing cabinet and is not accessed during the day to day running of FP.

Contact details of personnel will not be passed on to anyone outside FP without their explicit consent.

A copy of personnel contact details will be kept in the Emergency File for Health and Safety purposes to be used in emergency situations e.g. fire/ bomb evacuations.

Personnel will be supplied with a copy of their personal data held by FP if a request is made.

All confidential post must be opened by the addressee only.

Accuracy

FP will take reasonable steps to keep personal data up to date and accurate. Personal data will be stored for 6 years after involvement with FP and brief details for longer. Unless FP is specifically asked by an individual to destroy their details it will normally keep them on file for future reference. The Directors have responsibility for destroying personnel files.

Storage

Personal data is kept in paper-based systems and on a password-protected computer system. Every effort is made to ensure that paper-based data are stored in organised and secure systems.

Use of Photographs

Where practicable, FP will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), FP will remove any photograph if a complaint is received. This policy also applies to photographs published on the FP website or in any Newsletters.

B. External data records

Purposes

FP obtains personal data (such as names, addresses, and phone numbers) from clients, partners, venue providers and other contacts. This data is obtained, stored and processed solely to assist personnel in the efficient running of services. Personal details supplied are only used to send material that is potentially useful.

FP obtains personal data and information from clients, partners, venue providers and other contacts in order to provide services. This data is stored and processed only for the purposes outlined in communications with FP.

Consent

Personal data is collected over the phone and using other methods such as e-mail. Written consent is not requested as it is assumed that the consent has been granted when an individual freely gives their own details.

Personal data will not be passed on to anyone outside FP without explicit consent from the data owner unless there is a legal duty of disclosure under other legislation, in which case the Directors and relevant personnel. Contact details held by FP may be made available to groups/ individuals outside of the organization, but only with the verbal or written consent of those concerned.

Access

Only FP personnel will normally have access to personal data. All personnel are made aware of the Data Protection Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.

Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service. Information will not be passed on to anyone outside FP without their explicit consent, excluding statutory bodies e.g. the Inland Revenue.

Individuals will be supplied with a copy of any of their personal data held by the organisation if a request is made.

All confidential post must be opened by the addressee only.

Accuracy

FP will take reasonable steps to keep personal data up to date and accurate.

Personal data will be stored for as long as the data owner uses our services and normally longer. Where an individual ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed according to the schedule in Appendix B. However, unless we are specifically asked by an individual to destroy their details, we will normally keep them on file for future reference.

If a request is received from an organisation/ individual to destroy their records, we will remove their details and request that all staff holding paper or electronic details for the organisation destroy them. This work will be carried out by the Information Officer or Directors.

This procedure applies if FP is informed that an organisation ceases to exist.

Storage

Personal data may be kept in paper-based systems and on a password-protected computer system. Paper-based data are stored in organised and secure systems.

Use of Photographs

Where practicable, FP will seek consent of individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), FP will remove any photograph if a complaint is received. This policy also applies to photographs published on the FP website or in any Newsletters.

5. Disclosure and Barring Service

FP will act in accordance with the DBS's code of practice.

Copies of disclosures are kept for no longer than is required. In most cases this is no longer than 6 months in accordance with the CRB Code of Practice. There may be circumstance where it is deemed appropriate to exceed this limit e.g. in the case of disputes.

6. Responsibilities of personnel

During the course of their duties with FP, personnel will be dealing with information such as names/addresses/phone numbers/e-mail addresses of members/clients/volunteers. They may be told or overhear sensitive information while working for FP.

The Data Protection Act (1988) gives specific guidance on how this information should be dealt with. In short to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Staff, paid or unpaid must abide by this policy.

7. Compliance

Compliance with the Act is the responsibility of all staff, paid or unpaid. FP will regard any unlawful breach of any provision of the Act by any staff, paid or unpaid, as a serious matter which will result in disciplinary action. Any such breach could also lead to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy statement should be referred to the directors and in the first instance, to Wendy Lomas.

8. Retention of Data

No documents will be stored for longer than is necessary. All documents containing personal data will be disposed of securely in accordance with the Data Protection principles.

9. Communicating and reviewing the policy

FP will communicate awareness of the Data Protection Policy through the following means:

- Copies of all policies will be emailed to all personnel new and old
- A list of policies will be posted on the website (www.fizzypig.org) and the documents will be available by email.
- All personnel will be reminded that they must confirm with this policy on a regular basis.

This policy will be reviewed by the board, every 3 years or when there are changes in legislation.