FZY Data Protection & Privacy Policy

Policy

In line with the Data Protection Act 1998 and by the General Data Protection Regulations (GDPR) it is FZY's policy to ensure that information held is relevant, accurate and adequate; is not disclosed to third parties without express consent; is processed fairly and lawfully; is stored safely; is available to individuals on request within reasonable timescales, and not held for longer than is necessary.

Definitions

"FZY" means the unincorporated associated which goes by the name Federation of Zionist Youth or its acronym FZY and is a Jewish, Zionist, and Pluralist community youth movement. FZY is located at 25 The Burroughs, Hendon, London NW4 4AR and can be contacted via email at office@fzy.org.uk or by telephone at +44 (0)20 8201 6661.

"FFZY" means the Friends of FZY based at 25 The Burroughs, Hendon, London NW4 4AR. FFZY are a registered UK charity (261241) whose objects are set out in its trust deed and comprise the promotion of Jewish education and/or secular education among Jewish youth in the United Kingdom and Israel and in particular among members of the Federation of Zionist Youth (FZY).

"Members" means all the participants, applicants and their parent(s)/guardian(s) that have been on or applied to at least one FZY programme.

"Donors" means all the individuals who have donated money and/or assets to FZY, either directly or vicariously through FFZY.

"Volunteers" means all the people who are currently and have previously volunteered their time free of payment to FZY or FFZY often in, but not restricted to, a leadership capacity.

"Movement Workers" means all the persons who are or have been a sabbatical employee of FZY working a minimum of 20 hours a week for a minimum of a 6-month period.

"Staff" means all the people who are or have been employed by FZY either as a Movement Worker or in another capacity.

"Community" means all the people that fall within the Members, Donors, Volunteers, Movement Workers and Staff definitions as set out above.

What is confidential data?

Data is considered confidential if it contains the following material or similar;

- Personal data, as defined by the General Data Protection Regulations (GDPR), meaning any information relating to an identified or identifiable natural person.

- Sensitive personal data, as defined by the Data Protection Act 1998 and by the General Data Protection Regulations (GDPR), covering racial or ethnic origin, political opinions, religious or

philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health, sexual life, or details of criminal offences.

- Data relating to financial activities.
- Data relating to disciplinary proceedings, medical and welfare history, and harassment claims.
- Records containing "private" personal data, such as information relating to an individual's home or family life, personal finances, or a personal reference;
- Records of a commercially sensitive nature, such as contracts, tenders, purchasing and maintenance records, or legal documents.

FZY has both written and electronic documents that contain confidential data. Confidential data may be found in filing cabinets, drawers, desks, computers, servers, cloud storage systems and other reasonable places according to the policy directives below.

Why does FZY collect and process personal data?

FZY collects and processes data if one or more of the following apply:

- Consent has been given;
- It is necessary to fulfil a contract or agreement with an individual or organisation;
- To enter into a contract or agreement with an individual or organisation who has shown an interest in entering a contract or agreement;
- FZY has a legitimate interest in collecting and processing data to promote and deliver its programmes, activities and campaigns;
- The collecting and processing of data is carried out as part of FZY's legitimate activities as a not-for-profit unincorporated associated with religious and political aims;
- There is a legal obligation to collect and/or process data.

Personal data will be collected, processed and retained to enable FZY to:

- Achieve its mission and vision as outlined in FZY's constitution;
- Deliver, promote, inform and improve its activities, programmes and campaigns;
- Communicate should an important or emergency arise;
- Communicate about programmes, activities and campaigns that its Community have registered to or expressed an interest in;
- Communicate about other programmes, activities and campaigns FZY offers;

- Monitor and assess the needs of its Community to make changes to its programmes, activities and campaigns when needed;
- Raise necessary funds;
- Pay people and/or organisations when required;
- Record accidents and incidents;
- Comply with legislation.

How does FZY collect personal data?

In many scenarios the choice is with the individual as to whether to provide FZY with personal information. In certain situations, an individual will not have the option to opt out, for example, when FZY are delivering a programme, activity or campaign that was signed up for.

There are numerous ways FZY's Community may be providing information to FZY. These may include but are not limited to:

- Starting an application form for an FZY programme, activity or campaign;
- Making a booking or reservation for a programme and activity;
- Subscribing to FZY's email or postal mail distribution list;
- Contacting FZY with an enquiry;
- Joining an FZY or FFZY led or supported campaign;
- Completing a survey which contains your personal information;
- Forwarding an email sent by FZY's email distribution list to another email address;
- Entering a competition;
- Reporting a problem;
- Purchasing merchandise.

How does FZY use personal data collected?

FZY uses personal data collected to maintain accurate internal records of its engagement with its Community. These records facilitate FZY's programming, activities and campaigns run in accordance with its mission and vision statements as outlined in its constitution. Personal data also enables the processes in which FZY raises funds and awareness about its work. There are times when personal data may be processed and viewed by relevant Staff and Volunteers. All these Staff and Volunteers will be made aware of this policy and will need to work in accordance with it.

FZY may use personal data to send information about matters relating to FZY's programmes, activities and campaigns which may be of interest to its Community.

There may be times FZY will need to share personal date with third parties. This will only be done with trusted third parties and once FZY are satisfied that all data will be kept private and secure to the standards set by the Data Protection Act 1998 and the General Data Protection Regulations (GDPR). Any transfer of data will be in accordance with this data protection and privacy policy (see below for section on sharing and disclosing data).

What data does FZY collect, how is it maintained and for how long is it stored?

The section below outlines the personal data FZY collects, stores and processes from the different groups of people it interacts with. By each category of data, the length of time FZY will store this piece of information it is noted unless FZY are required to store this longer for the purposes of legal compliances.

Members and Volunteers

The personal data collected, stored and processed includes, but is not limited to, information to:

- Identify Members and Volunteers to ensure eligibility to be part of the FZY Community and to communicate about FZY programmes, activities and campaigns: Name [50 years post participation]; Date of birth [10 years post participation]; Basic contact details, i.e. telephone number, mobile number, email address, postal address [50 years post participation]; Organisational involvement [50 years post participation].

- Successfully deliver FZY programmes, activities and campaigns: Gender [10 years post participation]; Religion and synagogue affiliation [10 years post participation]; Passport copies and information [10 years post participation]; Emergency contact details [10 years post participation]; Occupation [10 years post participation]; Health and welfare, i.e. disabilities, medical conditions, vaccination history, additional needs or support, etc [10 years post participation]; Activity information, i.e. attendance history, discipline record, etc [10 years post participation]; Disclosure and Barring Service (DBS) report [50 years post participation]; Swimming ability [10 years post participation]; Programme, activity or campaign preferences , i.e. t-shirt size, rooming requests, travel preferences, add-ons or chuggim (extra-curricular) preferences, etc [10 years post participation]; References [10 years post participation]; Educational background, qualifications and awards [10 years post participation].

- Improve the promotion and delivery of FZY programmes, activities and campaigns: Surveys and interviews [10 years post participation]; Feedback on activities [10 years post participation]; Suggestions for future improvement [10 years post participation].

Donors and Partners

The personal data collected, stored and processed includes, but is not limited to, information to:

- Successfully communicate with Donors and Partners to ensure they are up-to-date with FZY programmes, activities and campaigns: Name [7 years post donation]; Date of birth [2 years

post donation]; Basic contact details, i.e. telephone number, mobile number, email address, postal address [7 years post donation]; Organisational involvement [7 years post donation].

- Maintain and increase donations for FZY either directly or vicariously through FFZY: Donation history [7 years post donation]; Donation preferences [7 years post donation].

Staff

The personal data collected, stored and processed includes, but is not limited to, information to:

Identify employees and to ensure their eligibility to work for FZY: Name and title [50 years post-employment termination]; Address and telephone number [50 years post-employment termination]; Payroll number [7 years post-employment termination]; Date of birth/age [7 years post-employment termination]; Disclosure and Barring Service (DBS) report [50 years post-employment termination]; Copy of passport [7 years post-employment termination].

Pay employees and allocate employment costs correctly: Job title, location and budget code [7 years post-employment termination]; NI number and tax code [7 years post-employment termination]; Payments and deductions made [7 years post-employment termination]; Bank details [7 years post-employment termination]; Hours worked and attendance [7 years post-employment termination]; Retirement and pension records [Permanent].

Enable FZY to monitor the effectiveness of the organisation's equal opportunities policies: Sex [7 years post-employment termination]; Marital status [7 years post-employment termination]; Career history [7 years post-employment termination]; Ethnic origin [7 years post-employment termination]; Disability [7 years post-employment termination]; Religion [7 years post-employment termination].

Enable monitoring and ensure accurate application of terms and conditions of employment: Retirement age [7 years post-employment termination]; Notice period [7 years post-employment termination]; Previous employment with FZY [7 years post-employment termination]; Health check records [7 years post-employment termination]; Maternity details [7 years post-employment termination].

Contact someone close to an employee in the event of an emergency: Contact name and relationship to employee [7 years post-employment termination]; Address and telephone number(s) [7 years post-employment termination].

Facilitate discussions on performance: Attendance, i.e. sick absence certificates, doctor's reports [7 years post-employment termination]; Notes of performance review meetings/supervision meetings [7 years post-employment termination]; Training history [7 years post-employment termination]; Disciplinary warnings and penalties [7 years post-employment termination].

Payments (including donations)

The personal data collected, stored and processed includes, but is not limited to, information to:

Process payments received from and made to individuals and organisations: Card information or bank account details.

- All this information for online payments are passed directly to a card processor and is not stored by FZY.

- All this information provided directly to FZY, i.e. via telephone to make a payment, is passed immediately to the payment processor and then deleted or destroyed in accordance to FZY's policies (see below).

- FZY strongly discourages the submission of card details via email.

Suppression Lists

To ensure the rights of the individuals, FZY will keep a suppression list until further notice to ensure it will not contact or process the data of those individuals that have requested FZY not to do so.

Data accuracy

FZY is legally required to take reasonable steps to ensure that data kept is accurate and up to date. Therefore:

- Staff should take every opportunity to ensure data is updated, i.e. confirming an individual's details when speaking with, having a form in a publicly accessible space for its Community to update contact details, etc.

- Data should be updated as inaccuracies are discovered, i.e. deleted from a postal address list if mail is returned, etc.

Website and cookies

FZY's website uses cookies. A cookie is a small file which asks permission to be placed on the hard drive of the computer accessing it. Once permission has been granted, a file is added, and the cookie helps analyse web traffic or lets an individual know when a website is visited. Cookies allow web applications to respond to the user. A web application can tailor its operations to the needs of the user, i.e. their likes and dislikes by gathering and remembering information about preferences.

FZY uses traffic log cookies to identify which pages are being used and what time of the day/year the website is being accessed. This helps FZY analyse data about web page traffic and improve its website to tailor it to the needs of the user. FZY only use the information provided by cookies for statistical analysis purposes.

A user can choose to accept or decline cookies. Most web browsers automatically accept cookies, but a user can normally modify their browser settings to decline cookies. By choosing this option, it may prevent the user from taking full advantage of the website.

FZY may also collect and store information about the browsing device of the user, including, where available, the IP address, operating system and browser type. This is anonymous statistical data about browsing activities and patterns and does not contain personal data.

Social Networking

Information that a user posts via social networking is generally accessible to, and may be collected by, others and may result in unwelcome communications. For reasons of safety and security users should not provide personal data on those areas of FZY's website or via FZY's social networking accounts. If a user does disclose any personal information via social networking, FZY does not accept any responsibility or liability for any breach of privacy, loss, damage, effect on the reputation of the user or otherwise whatsoever.

Links to other websites

FZY's website contains links to other websites of its partners and that may be of interest to the user. Once a user uses these links and leaves FZY site, FZY cannot be responsible for the information on these other websites or the protection and privacy of any information which the user provides whilst visiting such sites. As such, these websites are not governed by FZY's data protection and privacy policy. Users should exercise caution when on these other websites and it is advised to look at the data protection and privacy policy applicable to the website in question.

Data Storage

Storing confidential data within the work environment

Appropriate security measures must be implemented to protect all confidential data from unauthorised loss or accidental or deliberate damage. These measures include:

- Confidential data will be held in as few places as possible and Staff should attempt not to create any unnecessary data sets.
- Confidential data stored on paper must be kept in a secure place (i.e. locked filing cabinet, locked desk drawer, etc) where unauthorised people cannot see it;
- This confidential data may only be removed from its secure place when it is being used. When no longer required, all confidential data must be returned to a secure place;
- Keys to secure places must be stored appropriately in the workplace and may only be available to named individuals;
- No confidential data can be left where unauthorised people may see it, i.e. at a printer, on a desk, etc;
- All confidential data when desks are unattended must be securely stored, which includes locking computers;
- Computers must be logged off properly before leaving the premises;
- FZY computers, servers, cloud storage systems and other similar technology may only be used by an authorised person;
- Passwords must be kept confidential, changed regularly and of a strong nature, i.e. use of a mixture of numbers, lower case characters, upper case characters and symbols;

- Electronic confidential data can only be saved on the designated drives, servers and/or cloud storage systems, with at no time can confidential data be saved to personal or work computers;

- All servers, designated drives and cloud storage systems that contain confidential data and the computers where this data will be accessed from must be maintained by trained computer specialists and must be protected by a firewall and approved security software.

Taking out and storing confidential data outside the work environment

- Confidential data can only be taken out of the workplace by the direct consent and knowledge an employee's line manager and only for FZY business.

- No Volunteer, consultant or contract staff may remove confidential data from an FZY workplace without the express permission given by either the FZY Office Manager or FZY Executive Director.

- Confidential data may not be kept at home other than for FZY business and then only with the consent and knowledge of either the FZY Office Manager or FZY Executive Director and for a limited time only. This confidential data must be returned as soon as its purpose is finished.

- Confidential data must never be left in a car unattended.

- Reasonable care must be taken to ensure that confidential data outside of the workplace is held securely in a locked environment.

Storing confidential material for future use (archiving)

- Only FZY approved external archiving that has a secure and locked format is acceptable for use. Only the FZY Office Manager or FZY Executive Director can approve this storage.

Disposal of Confidential Material

- When confidential material is no longer required, the data must be appropriately destroyed, by shredding the documents or deleting them from the servers, designated drives and cloud storage systems. No other method of disposal of confidential data is acceptable.

Sharing and disclosing data

Which organisations or individuals could FZY share personal data with?

On specific occasions FZY may share personal data with trusted third parties once FZY are satisfied that any such use of data will be kept private and secure to the standards set by the Data Protection Act 1998 and the General Data Protection Regulations (GDPR). FZY need to share personal data where there are the following needs:

- To provide community partners, funders and programme operators the ability to deliver, promote, inform and improve FZY's programmes, activities and campaigns, and to monitor and assess the needs of the British Jewish community. UJIA, JAFI, Young Judaea Israel and Tzedek are current examples of trusted organisations where this sharing of data happens on a limited basis.;

- To communicate with its Community, i.e. through mailing companies for postal communications or through online platforms for email campaigns or newsletters;

- To process payments between FZY and its Community and its business partners, i.e. through online payment platforms and fundraising websites;

- To facilitate the delivery of programmes, activities and campaigns, i.e. information passed over to medical bodies and professionals;

- To promote events, news and campaigns that may be of interest to FZY's Community, i.e. a celebration of Israel's Independence Day or Hebrew classes;

- To comply with legislation, i.e. staff payment information to the Inland Revenue and pension company.

FZY will not sell or share personal data with any charities, businesses or marketing companies without the explicit consent of the individual except as stated above or for any other reasonable purpose to fulfil FZY's stated goals.

The sharing of personal data with trusted partners may involve information shared both within and outside of the European Economic Area (EEA).

All personal data must be password protected before being transferred electronically.

Before any personal data is shared, express permission must be given by either the FZY Office Manager or FZY Executive Director.

Rights of a data subject

Unless subject to an exemption under the General Data Protection Regulations (GDPR), a data subject has the following rights which this policy and FZY's use of personal data has been designed to uphold:

- The right to be informed about FZY's collection and use of personal data;

- The right to request a copy of the personal data which FZY holds about them;

- The right to rectification if any personal data FZY holds about them is inaccurate or incomplete;

- The right to request personal data on them is deleted where it is no longer necessary for FZY to retain such data;

- The right to prevent the processing their personal data;

- The right, where there is a dispute in relation to the accuracy or processing of their personal data, to request a restriction is placed on further processing;

- The right to object to FZY using their personal data for certain purposes; and

- The right to lodge a complaint with the Information Commissioners Office.

For further information about the rights of a data subject, please contact the Information Commissioner's Office.

Accessing Information

According to the rights of a data subject as noted above, FZY will provide any information in response to a request. Please contact FZY for more details at office@fzy.org.uk. Questions, comments and requests regarding this policy are welcomed and should be addressed to office@fzy.org.uk or to FZY, 25 The Burroughs, Hendon, London NW4 4AR or on +44 (0)20 8201 6661.

Roles & Responsibilities

All FZY Staff and many Volunteers with FZY have some responsibility for ensuring data is collected, stored and handled appropriately. Everyone that handles data must ensure that it is handled and processed in line with this policy and data protection principles. The following people have key areas of responsibility:

The Executive Director of FZY is responsible for:

- Reviewing all data protection procedures and policies in line with an agreed schedule;

- Handling data protection questions from Staff, Volunteers or anyone covered by this policy;

- Providing permission for a Volunteer, consultant or a member of Staff to remove confidential data from an FZY workplace and/or to store confidential data at home for a limited time;

- Checking and approving contracts with third-parties that may handle sensitive personal data;

- Providing approval for external archiving storage;

- Approving any data protection statements attached to communications such as emails and letters.

The FZY Office Manager is responsible for:

- Arranging any training necessary for Staff and Volunteers covered by this policy;

- Dealing with requests data access requests from data subjects to ensure FZY upholds these;

- Providing permission for a Volunteer, consultant or a member of Staff to remove confidential data from an FZY workplace and/or to store confidential data at home for a limited time;

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;

- Evaluating any third-party services FZY is using to store data, i.e. mass-email software;

- Providing approval for external archiving storage;

- Where necessary, working with Staff, Volunteers or others to ensure marketing initiatives abide by data protection principles.

Key Information

Policy prepared by: Joel Jacobs
This policy is effective from 25th May 2018
Next review: 25th May 2019

FZY may change this policy from time to time and any such changes will be published on its website. Notwithstanding any change to this policy, FZY will continue to process personal data in accordance with the rights of the data subject and FZY's obligations in law.