

FSSE Data Protection and Security Policy Data Statement

About FSSE

FSSE exists for the promotion and advance of the spiritual nurture and religious education of young people including both those of the Quaker tradition, and those with an interest in learning more about Quakers and Quakerism. This benefits personally the participants who attend the events, and also benefits the Religious Society of Friends (Quakers) more widely, through the spreading of Quaker ideas and ideals.

In carrying out these purposes, FSSE currently organises two annual residential Quaker events in August of each year: Junior Gathering (for young people aged 11-14) and Senior Conference (for older participants aged 15-18). These events benefit the young people who attend them enormously, by providing spiritual education through workshops which advocate the Quaker testimonies of peace, simplicity, equality and truth. The events provide spiritual nourishment from new (and old) friendships, shared worship and activities including sports, games, drama, music and other creative arts.

Principles of data handling

FSSE is not required to register with the Information Commissioner's Office as a not-for-profit organisation, although it adheres to the following 'data protection principles' set out in the GDPR Act, ensuring that all personal information collected is:

1. Used fairly and lawfully
2. Used for limited, specifically stated purposes
3. Used in a way that is adequate, relevant and not excessive
4. Accurate and up to date
5. Kept for no longer than is absolutely necessary
6. Handled according to people's data protection rights
7. Kept safe and secure
8. Not outside the European Economic Area unless that country or territory ensures an adequate level of protection

Our Data Protection policy:

- Ensures that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- Establishes appropriate retention periods for personal data
- Ensures data subjects' rights can be appropriately exercised and that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly
- Provides adequate security measures to protect personal data and sets out procedures for sharing
- Ensures that all staff are made aware of good practice in data protection and that there is adequate training for all staff responsible for personal data
- Ensures that everyone handling personal data knows where to find further guidance
- Will be reviewed on a regular basis

Nominated Officer:

The Clerk of FSSE is FSSE's nominated officer for data protection and any queries about data protection procedures should be directed to the Clerk at info@fsse.org.uk.

Retention and storage of data

In order to promote and advance spiritual nurture and religious education of young people including both those of the Quaker tradition, and those with an interest in learning more about Quakers and Quakerism, FSSE collects and stores data where subjects give permission and uses it for the purposes of organising the two summer events. We securely retain the following for as long as it is required in case of any historic safeguarding concerns being raised:

- Health and Safety Records (e.g. risk assessments)
- Child Protection Records
- First Aid Records
- Participant/Volunteer Lists
- Session records (ie. Timetable)
- Pastoral Concerns Records
- Participant Consent and Medical Information
- Volunteer References
- Volunteer DBS information

We will only get in touch with young people and volunteers about future events if they have given us explicit consent to do so.

Subjects may request that we destroy their data at any time. Data will always be stored securely and where practical, it will be kept in an anonymised form. Records of any personal data will be kept up to date in the 'Record of Data Held at FSSE' spreadsheet.

Data will be transferred in an encrypted form and stored in the online booking system in an encrypted database using separate passwords for each dataset. Where physical records of personal data are kept these will be kept in a locked cabinet during the event and then cross-shredded once the week is over. Data that needs to be held indefinitely (ie. Records of safeguarding incidents, timetable and staffing lists) will be archived securely.

Data subjects' rights and data/access queries

Where possible queries or requests for access from data subjects will be dealt with within a week by the member of staff initially contacted. Where further guidance is needed queries will be passed on to the Data Controller. If a period of more than a week is needed, subjects will be informed as to the reason for the delay and given an estimated period within which their query will be answered.

All booking forms and volunteer application forms inform recipients of who to contact if they have any queries about their data. Privacy notices will comply with guidance [provided by the ICO](#). They will also state that data will be stored and processed and their rights protected in line with the data protection act.

Staff education and training

All staff will undertake data protection training on a regular basis. Data protection procedures, guidelines and training will also be reviewed regularly.

Data and IT security

As a small, volunteer-run charity, we have no central offices and therefore our data systems must be compliant, yet proportionate to the type of data we are collecting and the resources we have. We adhere to the following procedures:

- Application forms are completed on a secure server with a HTTPS connection. Once the form is submitted the data is then encrypted and stored in a database. The Bookings Secretary and Event Co-Ordinators have the password. Others who need access, such as Planning Co-Ordinators, can be given the password but this should only be transmitted by using another communication channel.
- When the data is downloaded from the bookings system it is again transferred to the person downloading over a HTTPS connection. Computers that hold this information must be secure through using the following measures:
 - A strong password (Such as one which is longer than 8 characters, does not contain common phrases or commonly used passwords such as "password" and contains some uppercase, lowercase letters and or numbers and special characters)
 - An up to date system (including browser)
 - A virus checker/firewall, such as [Norton](#)
 - If possible, an encrypted storage/disk. You can read more about how to do this [here](#).
- This bookings data should not be transmitted by, or stored on:
 - Email
 - Unprotected USB stick/CD/other medium with the file on
 - Using 3rd party file hosting services such as Google drive, Dropbox, OneDrive, Apple cloud backup etc
 - Shared/public computer and any other non-secure methods

As FSSE has no offices, internal network and everyone is a volunteer it is likely that for the purposes of running and organising the events that some data will be needed to be sent between people, for example a base group list. In these cases, the data should be redacted to only the data required (such as first name, initial) for the reasonable purpose thus removing extraneous personally identifiable or sensitive information.