



Data Protection Policy

Approved: 15th May 2021

Next Review: Winter 2022

This policy will be reviewed annually by the National Committee at the first full committee meeting of the year. This will include checking for any updates required by a change in local or national policy and legislation.

Purpose

This policy sets out the arrangements and responsibilities within Quest for meeting its duties in respect of data protection law.

It should be read in conjunction with Quest's **Privacy Policy** which can be found here:

G:\Shared drives\Our Constitution, Pol's, Job Dec's, Management Proc's & Prayers

Aims

Quest undertakes to respect individual privacy; and to only process personal data in accordance with the data processing principles set out in the GDPR. In particular, Quest will not process any personal data unless it has identified a legal basis on which to do so.

Accountability

The Quest Committee has responsibility for ensuring that Quest meets its legal duties as a data controller. Operational compliance is overseen by the Chair, other Committee members, and Regional Convenors. Quest will keep a record of all documentation that demonstrates compliance with data protection law, including data audits, data entry forms, subject access requests, complaints and reports on data security breaches.

Compliance with data protection law shall be an entry in Quest's risk register.

Procedures

Privacy risk assessments

All data processing operations will be audited to establish the nature of any personal data that is being processed, the purpose of the processing, the method in which it is processed; and the nature of any privacy risk associated with the processing. The information from the data audit will be used to identify a lawful basis for the data processing; to create and modify as appropriate, a

Privacy Policy (see below) for Quest; and to take appropriate measures to ensure the security of the personal data concerned.

Privacy policy

Quest's Privacy Policy will be published on the Quest website and will be drawn to an individual's attention whenever data is collected. This may involve publishing short privacy notices at the point of data collection, with a reference or link to the full policy.

Duration of data storage

Data will only be stored for as long as is needed; and in accordance with schedule set out in the Quest Standing Orders which can be found here:

G:\Shared drives\Our Constitution, Pol's, Job Dec's, Management Proc's & Prayers

Special category data

Quest collects demographic and equal opportunities monitoring information from members in order to provide appropriate services as well as to advocate and campaign on behalf of members. Some of this information is of a sensitive nature. Given that Quest exists to support LGBT+ Catholics, it has a legitimate interest in processing such data when an individual signs-up to become a member. For added privacy protection and to ensure that Quest complies with the law, the collection of this information also requires the consent of the individual.

Data sharing with third parties

As the Privacy Policy explains, Quest may share personal data with third parties in order to deliver its services. These providers are:

- 1) Cognito: to collect membership details, including equal opportunities monitoring information.
- 2) MailChimp: to provide email newsletters and circulars.
- 3) Zapier: to connect Cognito information to databases held on Google Workspace and to MailChimp.

- 4) Eventbrite: for processing attendance at events.
- 5) Third Party Printers to print and distribute paper mailings for example the bulletin.

The processing of data by these providers is or will be subject to written terms and conditions to which Quest agreed when it signed-up to use these services. Additionally, the providers are covered by their own privacy policies. In the event of third-party printers being used to distribute mailings the contract will require the deletion of shared contact information once the mailing is complete. The sharing of data will involve the use of secure and encrypted technologies to prevent data breach.

Personal data is also shared with HMRC to process Gift Aid information in accordance with current regulations.

Upholding the privacy rights of individuals

Quest will uphold the privacy rights of individuals. The procedure for raising a complaint is set out in our Privacy Policy. The complaint or request will be investigated; and where upheld, remedial action will be taken, and the individual concerned will be notified. If the complaint is not upheld or the request is refused, the chair will notify the individual in writing, explaining the reasons, and will advise them of their right to take-up the matter further with the Information Commissioner's Office.

Subject Access Requests will be considered, and arrangements made for the release of personal data, in accordance with the law.

Data security

Where Quest uses third party online providers to process personal data (see above: Data Sharing with Third Parties), we are confident that our agreements with them provide for storing data securely on their servers.

Any data stored on Quest devices; or devices used by Committee members and/or Regional Coordinators is protected by appropriate electronic security

measures; and can only be accessed by the individual user and within Google Workspace, our cloud-based intranet.

The security of personal information is monitored and reviewed at regular intervals by the Quest Committee.

Dealing with a data breach

All potential breaches of personal information are taken seriously; and will be investigated by a member of the Quest Committee without delay. The following procedure will be followed:

- 1) The investigation will consider whether the breach poses a risk to individuals, their rights and freedoms, including possible emotional distress, physical and/or material damage. If any of these are likely, those affected will be informed without delay.
- 2) Action will be taken at the earliest opportunity to mitigate the breach.
- 3) The Information Commissioner's Office and the Charity Commission will be notified within 72 hours of the breach, unless there is no risk to individual rights and freedoms.
- 4) A record of the breach and any subsequent actions taken will be recorded and reported to the Quest Committee.
- 5) Operating procedures and protocols, together with data security measures, will be reviewed and improved to prevent any further such breach.

Training

Quest will ensure that Committee members and Regional Coordinators responsible for processing personal information are appropriately trained.