Quaker Cloud Data Privacy and Security Policy

FGC is committed to keeping all data in the Quaker Cloud both private and secure. We use best practices, industry standards, and secure technologies to ensure that the information you're your meeting provides us with is used exclusively for the purposes you have contracted.

Ownership of data:

For copyright and intellectual property purposes, the Meeting is the sole owner of web pages, minutes, and membership lists submitted and posted by their members and attendees unless the content is a copy or derivative of work licensed by FGC under a Creative Commons agreement. If at any time your meeting decides to terminate its Cloud services, the meeting may request a complete copy of all meeting data, and further request that FGC delete all meeting data from the Quaker Cloud.

Access to data:

The following entities and individuals have access to the data submitted to the Quaker Cloud.

- **The general public** has access to all web pages, minutes, and other content that the meeting has designated "Public."
- **Members and attendees** of your meeting with login credentials have access to all web pages, minutes, and membership lists that the meeting has designated "Private," and can update or remove their own contact information at any time.
- **Logged-in members and attendees** of other meetings have access to all web pages, minutes, and membership lists that the meeting has designated shareable with other meetings and your meeting will have access to any such items that other meetings have so designated.
- **The meeting's Cloud Administrator(s)**, chosen by each meeting, have access to all web pages, minutes, and membership lists that the meeting has posted, and can alter or remove these at their discretion.
- **FGC Quaker Cloud staff** has access to all web pages, minutes, and membership lists that the meeting has posted, and can alter or remove these upon request.
    - The FGC privacy policy states that staff accessing data for any purpose other than to accomplish their job responsibilities is a violation of that privacy policy and can result in dismissal and legal consequences.

- FGC will not review, share, distribute, or reference for third parties any personal information except as may be required by law or as is necessary to protect the rights or property of FGC and/or our constituents.

- FGC does not share, sell, rent, or trade personally identifiable information with third parties for their promotional purposes.

- Contact information provided by a meeting to FGC through the meeting's use of the Cloud is only accessible to FGC staff tasked with supporting the Quaker Cloud and related systems. Staff that do not have a work-related responsibilities that requires access to this contact information do not haveaccess.

- **Third Party Services**: In order to provide Quaker Cloud services, FGC may share your meeting's data with companies and vendors that provide services that are integral to the Quaker Cloud. These companies do not sell, rent, or trade personally identifiable information with third parties. They do not use information provided by FGC for their promotional purposes or for any purpose other than to aid in FGC accomplishing its work.

Data Security

Your data is secure with the Quaker Cloud. The Quaker Cloud uses a variety of methods to ensure that your data is safe, secure, and available only to those people/organizations named in the Quaker Cloud Agreement and Contract

The Quaker Cloud utilizes some of the most advanced technology for Internet security available today. When you access our site using a supported web browser, Secure Socket Layer (SSL) technology protects your information using both server authentication and data encryption. When you log in, you will see a small lock icon at the bottom of your browser display, indicating that a secure connection has been established to our server.

The Quaker Cloud Salesforce.com provides each user in your organization with a unique username and password that must be entered each time a user logs in. Salesforce.com issues a session "cookie" only to record encrypted authentication information for the duration of a specific session. The session "cookie" does not include either the username or password of the user. Salesforce.com does not use "cookies" to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

In addition, the Quaker Cloud is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders. All customer data is backed up on tape on a nightly basis, up to the last committed transaction. The Quaker Cloud further enhances our reliability measures by storing all customer data on mirrored disks that are mirrored across different storage cabinets and controllers. We are taking extremes to ensure your data will not be lost

As outlined in the FGC Privacy Statement, the Quaker Cloud does not review, share, distribute, print, or reference your data except as provided in the Quaker Cloud Agreement and Contract, or as may be required by law. For exact information, please refer to the Privacy Statement, as well as the Quaker Cloud Agreement and Contract.

In addition, the Quaker Cloud is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders. All customer data is backed up securely to the cloud on a nightly basis, up to the last committed transaction, and retained for 30 days.

- Backups: Backups: The database and file-system for the Quaker Cloud are backed up nightly. These backups are retained one month on secure cloud servers. The code base is stored in version control on secure cloud servers as well.

- Password encryption: Because people reuse their passwords on multiple services, the single most valuable piece of data FGC stores is the email address/password pairs created by member/attendees logging in. As a result, passwords are the most securely stored piece of data – it would require the fastest computers in the world several times the life of the universe to decrypt a reasonably strong password in use for the Quaker Cloud. Password hashes are created using 16385 iterations of SHA- 512 hash with individualized salt for each user. This means that a rainbow table, the most common tool to decrypt this data, is useless. Furthermore, FGC staff with administrative access have passwords that are 14-character long pseudo-random strings including uppercase, lowercase, numbers and symbols.

- Security of data in transit: All Quaker Cloud data is protected in transit via SSL/TLS