Leeds Area Quaker Meeting

of The Religious Society Of Friends

Registered Charity 1134542

IT Policy

This policy supports Leeds Area Quaker Meeting (LAQM) staff and volunteers in fulfilling our responsibilities in relation to IT security, including data security. It covers the use of, and access to, IT resources provided by LAQM for staff and volunteers for the conduct of LAQM business - principally the LAQM email addresses and cloud storage. It does not cover all uses of personal IT resources by volunteers to support LAQM's work, but volunteers are encouraged to follow the good practice it sets out. The policy should be read in conjunction with Britain Yearly Meeting's data protection policy (which LAQM follows), with the LAQM data protection and consent form, and with other relevant guidance on the protection of personal data.

Data Storage & email

It is important to ensure that data is stored safely to prevent the loss of data from technical failure, accidental deletion and malicious damage. Data must also be stored securely, using systems and practices that reduce the chances of data breaches where data, including personal data relating to employees or members, could be compromised. All employees and role holders share responsibility for ensuring data is stored safely and in compliance with our legal obligations.

LAQM have chosen the Microsoft 365 platform for cloud storage of data and email. Staff and role holders with a need for an @leedsquakers.org.uk email address will be provided with an email account. These email accounts should not be considered private and personal the to individual, even if they are in the individual's name. Where appropriate LAQM may grant other users access to the account during periods of unavailability due to illness, situations where the individual is no longer associated with LAQM, there is a change of role holder or the original individual has had access revoked for any other reason. Users should therefore avoid conducting personal conversations unrelated to their LAQM role in their LAQM email account.

The use of personal email addresses as public facing points of contact and for official roles is discouraged as these can present a security risk and complicate the transition of roles between individuals.

Staff and role holders will be granted access only to the storage areas and email accounts that they need access to in order to fulfil their role.

Data should not be stored on any other cloud services or platforms without prior consent of the trustee responsible for IT matters.

Administrators should limit access to data such that each user has access only to the data and email accounts required to undertake the work assigned to them.

Passwords

Passwords used to access LAQM systems, and any other facilities where LAQM data is stored is stored, should be appropriately complex, containing a mixture of upper and lower case letters, numbers, and symbols, no shorter than 12 characters. Passwords must only be used for one application or service. Passwords should not be shared between users. Avoid predictable passwords and when updating passwords do not use a password that is in sequence with a previous one (Password1, Password2 …). A short phrase of unconnected words can be easier to remember than a traditional password.

Multi-Factor Authentication (MFA) must be used where it is available. Where MFA is not available consideration should be given as to if the facility in question is appropriate for the nature of data being stored. If the data is sensitive personal data and the system is cloud/hosted then it would not usually be appropriate for it to be stored on a system that did not support MFA. If there is doubt guidance should be sought from the LAQM trustee responsible for IT matters.

Use of personally owned devices

Employees will be advised of policies regarding use of personally owned equipment for data and email use, such as computers and mobile phones, appropriate to their role. In the absence of any advice to the contrary they should only use devices provided by their employer to access and maintain LAQM data and email.

Volunteers and other role holders will generally be expected to use their own equipment. That equipment must meet minimum criteria as follows:

- Operating system supported by the manufacturer for security updates
- Updates applied regularly to the operating system to ensure it has the latest security updates

- Antivirus software to be installed with active subscription for updates
- Data storage encryption to be supported and enabled
- Password or PIN required at start up

Data should only be stored on personally owned devices for such time as it is necessary, which in most circumstances would be the time that it is actively being worked on. At other times data should be stored on LAQMs cloud storage.

By using your own device you agree that in the event of an actual or suspected data breach LAQM or their contractors may have access to your device in order to risk access the incident and take steps to mitigate and risks to LAQM data. You may also be asked to demonstrate at any time that your devices are appropriate regardless of concerns relating to a specific data breach.

Incident response plan

If you believe that your LAQM Microsoft account or data stored on your device has been compromised, this should be reported immediately to trustee responsible for IT matters.

Approved by LAQM Trustees June 2026

Review Date July 2028