

Guidance for BYM committee members

General committee service

Using your own device for BYM committee work

Please ensure you are familiar with the BYM Information Security Policy available from www.quaker.org.uk/data-safety.

As a committee member, you will likely be using your own computer, laptop, tablet or mobile phone to manage papers and prepare for meetings and other related activities.

You should take precautions to ensure the security of the information you hold, in particular personal information which is subject to the Data Protection Act 1998 and General Data Protection Regulations 2016.

Due to the nature of our work, this personal information is considered to be particularly sensitive as it includes religious affiliation but may also identify age and other attributes that could cause the individual to be discriminated against.

Any loss of personal information, eg a lost laptop or paper file, or if your computer is infected by a virus or malware (especially if you have confidential files) must be reported to the BYM Data Protection Team immediately. Email dataprotection@quaker.org.uk

How should you protect the information you hold?

- Save as little as possible onto your local computer or mobile devices.
- Use the secure Committee Hub to access committee papers.
- Do not share your computer or mobile devices with others, or share your password.
- Do not include personal information within emails as they are not encrypted. Instead use password protected attachments or online facilities provided by BYM, eg the Committee Hub.
- Check emails before you forward them on in case there is sensitive information in the email trail below your message.
- Keep paper records filed and out of sight when not in use.
- Fully delete the information from your computer / mobile devices when you leave the committee.
- Destroy all paper records or return them to your committee secretary when you leave the committee.

Good practice in keeping your computer and other devices safe

- Encrypt your computer and mobile devices and use password protection.
- Use virus and malware checking software which is regularly updated.
- Use a strong but memorable password, at least 8 characters long, include letters, numbers and other characters, or three unusual words together – change annually.
- Do not write down your password and have it easy to find.
- Keep software and operating systems up to date.

Staying safe on the move

- Be wary of links solicited through text messages. They can be travel alerts, scare tactics or other urgent notifications that trick a user into installing mobile malware of spyware.
- Do not use untrusted phone chargers, they can be used to steal data.
- Stay off public Wi-Fi and use your own private hotspot.
- Disable all wireless services until you are actually using them.

For further information refer to the BYM Data Safety and Information Security on www.quaker.org.uk/data-safety or contact the BYM Data Protection Team at dataprotection@quaker.org.uk.

Data Protection and GDPR – for members of Nominating Committees

The information that you take from people breaks down into two broad categories:

- Names of Friends, addresses, telephone numbers
- Opinions about those Friends (much of it sensitive, some of it occasionally not relevant)

This is legitimate business (you need it to do the work required for nominating committees) you can ask for it and store it for the duration of the time that it will be useful.

However

- It is also information that people can ask to view at any time (only the information about themselves).
- It is information that you cannot share, unless you have informed the person who gave it to you who and how you will be sharing it and gained their consent to do so.
- It is information that you have a responsibility to store safely.
- It is information that you have a responsibility to dispose of safely when it no longer is appropriate to hold the information.

While it is legitimate business to hold this information you should still inform the Friend:

1. What you are going to use the information for
2. Who you are going to share the information with
3. How you will save the information
4. How long you will keep it for (if you use personal computing to store the data, explain this, if you only keep it in paper form, inform them where it is kept).
5. How they can withdraw permission and ask for the data to be deleted

So if you are having a phone conversation with a Friend you might say:

“I am talking to you about a Quaker who has named you as a supporting friend. I will be taking notes and then typing them up and sharing them with other members of the search group and Central Nominations Committee to help us in our discernment. Britain Yearly Meeting will keep a copy of my final report on their secure servers and in their records. I will keep those notes for my records

while I am a member of Central Nominations Committee but I will destroy them when they leave. If at any time you would like me to destroy this information then please contact me or nominations@quaker.org.uk.”

For further information refer to the BYM Data Safety and Information Security on www.quaker.org.uk/data-safety or contact the BYM Data Protection Team at dataprotection@quaker.org.uk.