Central England Quakers

Data Protection and Privacy

Guidance to Friends on good email practice

Introduction

In the conduct of their business affairs, Friends are unusual in that they communicate almost exclusively via personal email addresses. In most business scenarios employees or volunteers tend to have business email addresses, and are able to communicate via secure email systems, without disclosing or compromising their personal addresses.

This reliance on personal addresses, in the context of the new General Data Protection Regulation, requires us to be especially careful over the way we use and share our addresses.

Also, one of the most common causes of "data breaches" (actions leading to the disclosure of personal data) is inadvertent email error – sending an email to the wrong recipient, attaching the wrong document, including inappropriate information in an email "trail", or disclosing personal addresses without consent when replying to or forwarding emails.

These guidelines are intended to minimise risk.

Guidelines

1 When sending an email always check carefully before pressing "send".

- Have you used the correct email address? (Some email systems "self-complete" addresses, and it is all too easy for the computer to select the wrong address)
- Have you attached the correct document(s)?
- Is there anything attached to the email (or included in a "trail" below) which is inappropriate for the new recipients?
- Which email addresses will be visible to the recipient(s) and do you have consent to disclose them?

2 If you are Convenor of a committee or group which communicates by email, check with the members that they are willing to disclose their addresses *within the group*, by "open circulation". If any object, ensure that their wishes are respected and include them as "blind copy" (bcc).

3 When replying to or forwarding emails you need to ensure that you have the consent of any visible "addressees" to disclose their addresses to any new recipients. If in doubt remove the visible addresses – it is easy to do this, when replying or forwarding, by marking and deleting the previous email address list.

4 Try to avoid building up long email "trails" – is the historical "trail" essential to the message, or are you just being lazy?! Keep the trails as short as possible by deleting any that are not essential or relevant. As advised in 1 above, browse through the trail, before sending the email, to ensure that it does not contain inappropriate content or compromise privacy of personal data.

5 Follow the rule of "one subject, one email" – try to avoid covering more than one topic in an email. This not only makes filing and retrieval easier, but also reduces the risk of disclosing inappropriate or unnecessary information if the email is shared. Also check that the text in the "subject" line is correct for the content.

6 If you are asked for an individual's email address, never disclose it without the consent of the individual. It may be helpful to offer to contact the individual and ask them to contact the enquirer. (NB the same rule applies to telephone numbers and postal addresses).

7 When sending newsletters or other general communications to members or attenders by email, always circulate by "blind copy" (bcc). This will protect the anonymity of those on the mailing list. Make sure that you have the consent of recipients to send them such mailings, and give recipients the opportunity to "unsubscribe" at any time.

Published by the CEQ IT and Data Protection Committee, June 2018