



Data Safety and Information Security

Guidance for meetings

A link to an electronic copy of this document is available at
www.quaker.org.uk/clerks

Fourth edition, 2014

This replaces all previous editions

Published by Quaker Communication and Services Department, Friends House,
173 Euston Road, London NW1 2BJ

Table of contents

Introduction	2
Guidance for meetings and committees	4
Policies and compliance	4
Data Protection registration	4
Responsibilities of meetings, committees and staff	5
Asking other organisations to work with data we hold	5
Frequently asked questions	7
List of contacts at Friends House	15
<i>Quaker faith & practice</i> on data protection and confidentiality.....	16
Appendix 1: Information Security and Data Protection policies	17
Britain Yearly Meeting's Information Security Policy	17
Appendix 2: Sample forms and examples	24
Example of the area meeting compliance questions.....	24
Summary of Quaker Data Safety and Information Security	25
How your information is used, with your consent.....	25
Sample data consent form for a meeting	26
Appendix 3: QList – an online facility for meeting membership lists.....	27

Introduction

Our religious Quaker community is underpinned by openness and mutual accountability to one another. As Friends we seek to be clear and transparent in the work that we do, in the methods we use, and in our recording and reporting on our processes and achievements.

Just as we expect that personal information about ourselves is properly protected by the other members of our meetings, committees and by the staff of Britain Yearly Meeting (BYM) who have authority to use it, we all also need to observe the requirements of information and data protection legislation.

BYM, many area meetings and some regional meetings have registered as individual charities. Other area meetings, as their income reaches the current threshold of £100,000, will also register. Each registered charity becomes responsible for its own data safety; however until that time, their data records remain covered by the Yearly Meeting's original central registration under the Data Protection Act 1998.

Our central registration continues to cover data held by other constituent parts of Britain Yearly Meeting, including central and other standing committees. Regional general meetings which are not part of the BYM administrative structure are no longer covered by our central registration (see [page 4](#)).

Clerks and committee members need to be familiar with the basic requirements of the Act and of Britain Yearly Meeting's policies on information security and data protection (see [page 17](#)), which Meeting for Sufferings Committee agreed on behalf of Meeting for Sufferings (July 2003 minute 5).

This booklet includes frequently asked questions ([see page 7](#)) based on queries raised by meetings. On [page 25](#) is a summary of the implications of the Data Protection Act for meetings which can be displayed in the meeting house or used to tell members and attenders about data protection.

To start, the most important items of information to remember are the key principles of the Act:

The 8 basic principles of the Data Protection Act (1998):

1. Personal data shall be processed fairly and lawfully in accordance with the Act.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This guidance will go into the Act in more detail, with specific examples of how it applies to meeting records, but these principles should guide everything we do.

Guidance for meetings and committees

Policies and compliance

The policies and procedures are commended for the use of the meetings and committees of the Yearly Meeting, for inclusion in handbooks for Meeting for Sufferings and committees and for circulation to their clerks and the clerks of other bodies within the Yearly Meeting for their use.

They are intended to help minimise the compliance process within the Yearly Meeting, and to reduce the burden on its clerks, and the clerks of its constituent meetings and committees in reporting on implementation of the policies.

Good practice requires us to keep confidential some categories of information, and these are listed in the BYM Information Security Policy appendix (page 18).

Data Protection registration

Following the decision by the charity commissioners to end the excepted status for religious charities, BYM and its larger meetings are registering as individual charities with the Charity Commissioners. Each charity becomes responsible for its own data safety and BYM recommends that they each notify the information commissioner to register with his office.

The two registrations are separate – firstly the registration as a charity with the charity commission www.charity-commission.gov.uk and secondly the notification to the information commissioner's office to register as a data controller http://ico.org.uk/for_organisations/data_protection/registration.

Until a meeting becomes a separate charity, its data records remain covered by the Yearly Meeting's original central registration under the Data Protection Act (1998). Our central registration also continues to cover data held by other constituent parts of Britain Yearly Meeting, including central and other standing committees.

The eighteen regional general meetings in England and Wales were removed from the administrative structure of BYM in 2007 and are no longer covered by our central registration. Meetings which remain within our administrative structure (other regional meetings, area meetings and their associated local meetings) are covered by our central registration until such time as they register as independent charities. Until then, they are not required to make their own submission to the Commissioner or appoint their own compliance officer.

As the Data Compliance Officer for the Yearly Meeting, the Recording Clerk is responsible for ensuring the Yearly Meeting conforms to the Data Protection Act 1998. The Recording Clerk will write to the clerks of all the AMs which are part of the BYM administrative structure annually, asking them to complete a compliance form. Reports can then be made to Trustees and thereafter to Yearly

Meeting. There is an example of the compliance form on [page 24](#).

Responsibilities of meetings, committees and staff

It is good practice for meetings or committees to designate an officer with responsibility to ensure understanding of and adherence to these policies, to serve as a point of contact or advice for members with queries and to return the compliance form to the Recording Clerk.

Contact information about members may be used by the constituent bodies of the Yearly Meeting for their legitimate business. It is accepted that lists of committee members' contact information may also be used to help members contact one another and be shared with other central or standing committees as appropriate to facilitate the centrally managed work. Information on attenders and non-member partners may also be held but used only with their explicit consent. Information on children and young people under 18 may only be used with the consent of their parents or guardians.

All members of BYM have a responsibility to protect personal information that they collect. This includes contact lists, books of members, papers, electronic files and information held by your meeting, committee, staff or passed to other organisations.

You are responsible for ensuring that the principles of data protection are observed if you delegate responsibility for maintaining a membership or mailing list or other records or for completing the compliance form to another person – a member of the meeting, committee or to staff. If you ask another organisation to use the personal details that you hold, for example to produce an address list or a mailing, you need to make it clear to them what they can and cannot do with the information that you provide to them (see the next section for an example).

If you, or staff or volunteers working on your behalf, hold and use other information on members and attenders, whether electronically or in paper-based records (for example in connection with nominations work, applications for membership, or eldership or oversight matters) the people concerned may see and approve their own record (see *Access to data* on [page 21](#)).

Employees of Britain Yearly Meeting are not permitted to give out your details or details of other members or attenders without their consent (unless the details are in the public domain already, for example in the *Book of Meetings*).

The Data Protection Act means that it is not possible for area meetings to send copies of their contact lists to Woodbrooke, to The Friend, to FWCC, or to any other organisations, without the consent of the individuals on that list. The sample consent form on [page 26](#) now includes a request for that consent.

Asking other organisations to work with data we hold

When we pass on the contact details that have been given to us, we have the

responsibility to make clear what can and cannot be done with them. For example, many Quaker meetings produce printed contact lists (books of members and attenders) which are sometimes compiled by individuals or organisations (such as general meetings or regional bodies) external to the meeting.

We recommend the good practice set out in the following paragraphs, which can serve as a model for the development of a solution. In all cases it is important that the basic principles of data protection (as set out earlier in this document) are followed. Individual circumstances will mean that individual solutions will be needed for each meeting.

When developing individual solutions, meetings should consider the security of personal details, the accuracy of these details and the expectations of those who have supplied the details. Solutions should be reviewed regularly and may need gradual development and improvement.

Example solution for contact lists compiled by another body

An organisation that collects personal information is termed the data controller of that information and responsible for it. Each part of BYM that collects and uses personal details shares in that responsibility. If you ask another organisation (Quaker or third party) to use the personal details that you hold, for example to produce your contact list, you need to make it clear what the other organisation can and cannot do with the information that you provide to them.

We recommend a simple mutual agreement or protocol be used to make the expectations of the data controller clear. The protocol will require adaptation for individual circumstances.

As an example for publishing a contact list a protocol might state:

"XXXXXXXXXXXX area meeting is requesting yyyyyyyyyyyyyyy to produce a printed list of contacts as agreed separately.

XXXXXXXXXXXX area meeting agrees that yyyyyyyyyyyyyyy will approach the area membership clerk and the local meeting clerks to obtain accurate contact details to be included in the published list. These details will include members, attenders, family members, children and young people. No dates of birth will be included in the published list. Individual email addresses for those under 16 will not be published (as advised by Meeting for Sufferings minute 3 (d), July 2003).

XXXXXXXXXXXX area meeting requires yyyyyyyyyyyyyyy to take reasonable precautions to keep the supplied details confidential and to prevent the contact details falling into the wrong hands. The use of mobile media (such as memory sticks) to store details should be kept to a minimum. The Quaker Communication & Services Department at Friends House (email webteam@quaker.org.uk) can offer advice about security and encryption for electronic media.

When obtaining the contact details, yyyyyyyyyyyyyyy will verify with the individuals supplying lists of details that the contacts on the list are aware that their details will be included and that they have had an opportunity to request that their details are withheld. Yyyyyyyyyyyyyyy will clarify with each clerk whether the list they supply includes these deletions of details or if yyyyyyyyyyyyyyy is expected to make deletions before publication.

Yyyyyyyyyyyyyyy will only use the supplied details for the purpose of producing the agreed list of contacts and will not pass them on to any other organisation."

Frequently asked questions

1. What are the basics to remember?

- Information about a person belongs to that person who has a right to say how it is used, and to know how it is going to be used.
- So, if you are compiling or using a list of people, you need to be sure everyone knows that they are included, knows what the list will be used for, and agrees to being on it.
- An organisation can hold basic details about its members, for example name, address, subscription, etc, and can use them for the reasonable administration of the organisation.
- If you ask for people's details, addresses, etc, for a particular occasion, for example organising a conference, this information should only be used by you for that purpose. If you are going to make further use of the information, particularly if it is to be passed on to others, then you must make this clear when collecting the information, or obtain permission before passing on the information.
- If an individual has given consent in the past for their details to be included on your contact lists, this consent continues until they notify you of a change (usually by completing a new consent form).

2. Does my meeting/committee have to register separately with the Information Commissioner?

No, not if your meeting/committee is still a constituent part of Britain Yearly Meeting (see Data Protection registration on [page 4](#) of this document and item 4 of the Data Protection policy on [page 20](#)).

BYM and those area and regional meetings that have registered with the Charity Commission are responsible for their own data safety. The data records of those meetings who are not yet eligible to register remain covered by the Yearly Meeting's original central registration under the Data Protection Act 1998. See [page 4](#) for further details about registration.

3. Why are area meetings not registered as charities with the Charity Commission asked to complete a data safety/data protection compliance form every year?

The Data Protection Act 1998 sets out rules for collecting, keeping and using personal information about living individuals. Any organisation in the UK that handles information about people must comply with it, and show that they are doing so. The compliance form (see sample on [page 24](#)) assists with this.

As the Data Compliance Officer for the Society, the Recording Clerk has to make sure that it is complying with the Act. At the conference of general and area meeting clerks in November 2003 at Woodbrooke it was agreed that a compliance form completed by each area meeting once a year was the best way to do this.

4. Do local meetings have to complete their own compliance form?

It was agreed at the conference of general and area meeting clerks in November 2003 that the compliance form would be completed at AM level, but AMs need to check what their local meetings are doing. It is for AMs to agree with local meetings how they do this.

5. To what lengths is the AM expected to go to confirm how data is handled by local meetings, committees, etc?

You need simply to ask what they do with personal information that they have, and how they comply with the Data Protection Act. The Society's Data Compliance Officer would encourage both AMs and local meetings to have data protection regularly on their agendas (e.g. annually) to keep the issue alive in Friends' minds.

6. What about visitors' reports for membership?

All those likely to take on this role should know of the importance of data protection. The *Summary of Quaker Data Safety and Information Security* (see [page 25](#)) gives a basic overview.

Visitors' reports should be factual and should not contain opinions about an individual, or any information which is likely to be confidential or sensitive. Applicants for membership may see what is written about them, and they often find it a very special and supportive document.

It is up to the AM to decide how long the reports should be kept. This will depend on whether the report is considered by the meeting to be purely for the purpose of deciding on an application for membership (resembling a job reference), or something precious. Anne Hosking, when she worked at Friends House, wrote guidance on this subject for an AM. For a copy please ask Helen Griffith (see [page 15](#)) for *Visits on Applicants for Membership*.

7. What is the difference between the register of members and a published contact list?

The official register of members includes only those in official membership and is only accessible to officers of the meeting and is for the running of the business of the meeting (see *Q&A* 11.37). The published contact list (or Book of Members) includes attenders and sometimes families, as well as members. It is more widely accessible and would normally be available to all those listed in it.

8. Do we need the consent of Friends to include their names on the register of members?

No.

Basic factual information on members such as their contact details can be kept on the official register of members without their consent. Such information may be passed to the Yearly Meeting's membership database, but members should be made aware that they can request that personal details other than their names be withheld (see *Q&A* 4.45). In general, members of an organisation must expect their details to be used for the legitimate and expected business of the organisation they belong to.

9. What written consent do we need from everyone whose name is included in the meeting's published contact list?

(a) Members:

If members are told that their details will be included in the contact list then this can be accepted as giving consent. You should tell members that you keep a contact list; that it is used for authorised purposes only, including the central contact database at Friends House; and it is kept in accordance with the Data Protection Act; and is not given to third parties. They can opt not to have their contact details (other than name) included in the contact list, printed in an address list or recorded on the Yearly Meeting central contact database by completing a consent form. Please note information on Qlist on [page 27](#).

When an individual is accepted into membership, they should be informed that their details will be kept in a contact list. You may wish to give them a copy of the summary on [page 25](#).

(b) Attenders and non-member spouses/partners of members:

Details of attenders and the non-member spouses/partners of members can be included only with their explicit consent.

(c) Children and young people under 18:

Details of children and young people under 18 may be included only with the explicit consent of their parent or guardian, but it is not advisable to identify children and young people separately in the contact list. E-mail addresses of children under 16 should not be published (Meeting for Sufferings, July 2003, minute 3 (d)). If elders, overseers, children's committees, etc. need to use dates of birth, then a separate contact list should be produced for them.

(d) Written consent:

We should be obtaining written consent by use of consent forms – see [page 26](#) for a sample. The consent form should allow people to indicate if there are details that they would like withheld from the local published list or not passed on for inclusion in the Yearly Meeting central membership database. The completed consent forms should be retained safely, usually by the editor of the contact list or the membership clerk(s). There is a sample form at the back of this booklet ([page 26](#)) that you can adapt for your own meeting's use. It may be useful to print the summary (on [page 25](#)) on the reverse of the form.

10. Do we need to obtain written consent every year to include a person's contact details in the published contact list?

No.

Once consent has been given it is deemed to last until it is specifically revoked. This can conveniently be explained on the consent form. It might be useful to include a blank copy of the form in the printed contact list to be used when contact details change or the person concerned wishes to change the availability of their data.

When a new attender is sufficiently part of the meeting for their contact information to be included on the contact list, then their consent is needed. They need to have explained to them what use will be made of the information they are giving.

If, at a later date, you plan to use the information for an additional purpose which is not part of the administration of BYM and not already included, then you do need to get individual consent for that new purpose.

11. What should we print in the published contact list or Book of Members about data protection?

A suggested form of words is:

“This list has been prepared in accordance with the Data Protection Act 1998.

It may be used by members of the Quaker meetings listed in it, for the administration of the affairs of the meetings and of any bodies set up by the area meeting, and for the legitimate purposes of the Religious Society of Friends in Britain. It may not be used for other purposes or by third parties.

Everyone on the list has agreed to the inclusion of their name and details, either by becoming a member of the area meeting or in writing.”

12. Someone has asked for information on contacts for Quaker meetings in a particular area – can we give them this?

If the information, for example the Clerk's name, is in the published Book of Meetings, then it is public information and can be passed on for the explicit purpose of contacting the individual (you should explain this when passing on the details). You cannot provide lists of information for other uses without having permission from the individuals on the list. If you have a problem with an enquirer asking for information which you would like to give but are unsure whether they can have it, you can consult with one of the contacts listed on [page 15](#).

13. Someone outside the meeting has asked for contact details of a particular Friend listed in my meeting's contact list – can we give them this?

No. You should take their details and pass them on to the Friend they are trying to contact or offer to forward a message so that the Friend can contact them.

14. What is the procedure when someone asks to see information held about themselves?

Guidance on the procedure for dealing with requests to see personal information is given in the appendix to the Data Protection Policy (see [page 22](#)). As a guide, if someone wishes to see personal data about themselves held by the Yearly Meeting then they should write to the Recording Clerk or to the relevant department. If they wish to see only data held by their local meeting or the area meeting, then they should write to the AM clerk.

The request has to be reasonable: they cannot expect you to search through every minute book for every mention of their name. It would be reasonable to specify minutes concerning them on a particular subject over a particular period. They may not see any minutes written about other people. If you have any queries when you receive a request for information, please contact one of the people listed on [page 15](#).

15. How does data protection affect visitors' books kept in meetings?

It depends on what the visitors' book is for and how you use it.

If it is for visitors to show they have been there and to write a comment, and for the meeting to just keep a tally on the number of visitors, then you don't need a space for their address and it can be left on display. Whether people write in it or not is voluntary, and so the Information Commissioner takes the view that people choose if they want to write in it, and the individual also decides how much personal detail they write – most just write their name, town/city where they live, their own Quaker meeting. We can all think of historic buildings, or non-Quaker events we've been to where we've filled in visitors' books and selected how much detail we write.

Some meetings think visitors' books are a way of inviting people to find out more about Quakerism and to collect contact details, for example, to send them details about Enquirer's gatherings or a Quaker event. If this is so, then you may want to re-think if this is a good way of outreach. Beth Allen wrote an article in *The Friend* (8 April 2005) about this, 'Welcoming those that seek us out'. Helen Griffith (see [page 15](#)) can send you a copy.

If you do use visitors' books for this purpose then you will be asking people to provide their contact details. In that case you should display a clear statement of how their details will be used and kept, and the visitors' book should not be left on display where others could access the details. Might it be more friendly to have plenty of leaflets that visitors can take away to read, and an attractive notice telling them who to contact if they would like to know more and inviting them to join Meeting for Worship?

16. Can personal details such as the names of recipients of grants be mentioned in Trustees' and Overseers' minutes?

Yes.

Following the provisions in the Data Protection Act doesn't mean we can't mention a person by name. For example, a meeting of AM trustees agreeing a grant will need to mention the names of the people to whom grants are given for necessary administration. The act of applying for a grant is considered to consent to the use of the details supplied in the application for the purposes of administering the grant.

Specific consent for such necessary administration as overseers' records, for example, does not need to be obtained from the people mentioned within them. Personal details of non-members who have not signed a consent form should not be mentioned in overseers' records except for the purposes of the necessary administration of the meeting. Provided the overseers' minute book is kept securely, the minutes record only the information necessary for the purpose and are circulated only to overseers who keep them safely, then the records are being kept and used legally.

17. How does the Freedom of Information Act relate to data protection?

The Data Protection Act sets out rules for processing and keeping personal information about living individuals, and applies to any organisation in the UK that handles information about people.

The Freedom of Information Act allows the public access to information held by public bodies but specifically excludes personal information. In any case as the Society is not a public body we are not obliged to make information or Quaker records public under the Act.

Following the guidance issued by The National Archives in July 2005, Quaker records held in a public repository are not affected by the Act because they are

held there on deposit and remain in the ownership of the area meeting. It is important that the Custodian of Records discuss the terms of deposit with the repository so they are fully understood and clear. There is guidance on how to deposit records on the BYM website under Support for Meetings > Records Custodians here: www.quaker.org.uk/records-custodians.

Please contact the library archivist at Friends House, Lisa McQuillan (see the List of contacts below), if you need further advice.

18. What about criminal records checks?

Detailed notes on the handling, use, retention and disposal of Disclosure information are available in the Churches' Child Protection Advisory Service (CCPAS) online manual Safe and Secure. See the In Focus section "Handling of Disclosure Information. Do note that this is only available to area meetings that belong to the CCPAS: trustees of area meetings that do not belong will need to obtain this information from other sources.

There is information about criminal records checks on the websites of the Disclosure and Barring Service (England and Wales) <https://www.gov.uk/disclosure-barring-service-check> and Disclosure Scotland <http://www.disclosurescotland.co.uk>.

19. What do I need to think about when using social media on behalf of Friends?

(a) Am I allowed to publish Friends names and contact details on social media?

As with printed materials, ask permission before you publish anybody's personal details. Keep a record of that agreement if you can. Remember that, depending on settings, contact details can be publicly accessible and pass hands much more quickly and easily than with printed matter.

(b) Can I share photographs of Friends on social media?

Take a great deal of caution when posting photographs of people. Ask people at the beginning of events if they mind having their photographs taken to be posted on social media. By its very nature social media makes it easy to identify and contact people. We'd advise that you don't share images of children on social media. Using children's images on a local meeting's Facebook page potentially identifies them and gives their geographical location.

(c) Tags, links and sharing

Remember that many social media sites make it easy for people to identify other people and connect. Take care that posts and photographs don't contain links to other people's pages or give away identifying details. Remember that if you allow comments and tagging on your content, all your best intentions for protecting people can be undone by a third person. Use privacy setting with care.

(d) Is my Facebook page private?

If you are using your own personal Facebook page to send messages to people in your meeting or share photos, you can make it private so that only people you are friends with can see your page and the content on it. This is all done through **Settings->Privacy**. You should also check the settings every time you upload photos as it will ask you who you want to share them with.

If you want to make a shared Facebook for your meeting you have two choices.

- You can make a 'Page', which is what brands, companies and public groups do – for example the Friends House Library (www.facebook.com/libraryofthesocietyoffriends) has a public page – this means anyone can view this page and the contents. This is good if you want to network widely, attract new users, advertise events, etc.
- The other option is to make a 'Group'. This means several people can be made administrators to share content among the group; however unlike a 'Page', you can choose some privacy options for a group. You can have an **open** group, so anyone on Facebook can see the content; you can have a **closed** group – this means anyone on Facebook can see the name, description, and members of your group, but only members can see the content (posts, comments, photos, etc); or you can have a **secret** group where all information about the group is only visible to the members. You can get information about setting up different kinds of accounts at www.facebook.com/help.

A group page is probably the most sensible choice if you want a meeting Facebook page.

Facebook change their privacy settings occasionally, so if privacy is important to your meeting, you should keep an eye on this. Usually there is quite a lot of press attention to any changes they make and a statement on the Facebook page.

20. How should I send an email to a group of people?

Before sending an email to a group of people using their personal email addresses you should consider whether it is appropriate to reveal all the email addresses to the recipients.

(a) If the email addresses are put in the 'To' or 'cc' (carbon copy) address boxes every recipient will see them and be able to send a reply to everyone. This may be appropriate for a small group of people that know each other.

(b) When sending email to a group of recipients who don't know each other's email addresses, use the 'Bcc' (blind carbon copy) address box so that the

recipients do not see all the addresses. Put your own address as the 'To' address box.

(c) Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

List of contacts at Friends House

Quaker Communication & Services (data compliance, data safety)

Helen Griffith
020 7663 1161
heleng@quaker.org.uk

Quaker Life (Criminal records, data safety)

Michael Booth
020 7663 1023
michaelsb@quaker.org.uk

Library (archives and records, data safety)

Lisa McQuillan
020 7663 1127
lisam@quaker.org.uk

The Data Compliance Officer is the Recording Clerk, Friends House, 173 Euston Road, London. NW1 2BJ

The Information Commissioner's Office (ICO) is the official body that oversees and enforces the Data Protection Act 1998. Its website www.ico.gov.uk has a great deal of general information and guidance for organisations.

The ICO have guidance on your right to access personal data on their website www.ico.gov.uk/upload/documents/library/data_protection/introductory/subject_access_rights.pdf and also offer a telephone helpline service on 08456 30 60 60 or 01625 54 57 45.

Quaker faith & practice **on data protection and confidentiality**

4.45 Meetings storing information about their members and attenders on computers or other electronic devices or in manually processed paper files should be sensitive to the need to protect such information from unauthorised use and must comply with all legal requirements for data protection. Basic factual information on members such as addresses can be kept by the area meeting on the official register of members (11.37) without notification of those concerned. Such information may be passed to the yearly meeting database, except that members may then request that information other than their names be withheld.

Information on attenders and the non-member partners of members may only be held with their explicit consent. Information on children not in membership (11.38) may only be held with the explicit consent of their parent or guardian. Consent forms for inclusion in the area meeting lists should be drafted to enable such persons to opt for their information to be passed on to the yearly meeting database.

Friends should be made aware of the difficulty of maintaining perfect security of the printed lists made available to members and, frequently, to attenders, and should be given the opportunity of deleting some or all of their personal details (11.39).

If meetings record any other information on members and attenders, whether electronically or in paper-based records, for example in connection with nominations work or with applications for membership, the persons concerned must be informed that the information is held and that they may see and approve their own record.

Further advice can be obtained from the Recording Clerk (see also 8.20).

(part of) 8.20

The Recording Clerk serves, for the purposes of the Data Protection Act 1998, as Data Compliance Officer and is responsible for ensuring that the recording and processing of data held by the Yearly Meeting conforms with the law (4.45).

Quaker faith & practice, fifth edition (revised 2013)

Appendix 1: Information Security and Data Protection policies

These policies were originally agreed by Meeting for Sufferings in July 2003, minute 5. The revised draft policies printed here have been updated in 2008 due to the changes in the constituent bodies of Britain Yearly Meeting and agreed by Trustees in March 2009, minute BYMT/09/03/13.

Britain Yearly Meeting's Information Security Policy

Everyone involved in the service of the Yearly Meeting has a duty of confidentiality to the Yearly Meeting and is required to protect information which:

- Is held in confidence, particularly any information which includes details held by the Yearly Meeting about individuals, such as nominations details.
- Is intended for restricted use, such as payroll or personnel information which is kept for management purposes only.
- May represent the intellectual capital of the Yearly Meeting, for example the results of research not yet approved for publication.

The duty of confidentiality remains after leaving the Yearly Meeting's service.

A list of information which is likely to be available to members and to the public or which is restricted is given in the Policy Appendix which follows this section.

Nothing in this policy should be taken as overriding existing statutory or common law obligations to keep confidential, or, in appropriate cases, to disclose certain information.

Information and records archived and transferred to the Library at Friends House that fall within the 'closed period' will normally only be available to the originating department. The 'closed period' for public access to BYM central records is 50 years and there is restricted access to any file containing information less than 50 years old. Public access to those files can be authorised only by the head of department. The Assistant Recording Clerk and the Librarian can also authorise access to closed files and the Recording Clerk can hear appeals raised by those who have not been given access.

The clerk of Meeting for Sufferings will act as arbiter when members of Meeting for Sufferings or Britain Yearly Meeting Trustees have not been given access to papers they have requested.

Information Security Policy - Appendix

Access to information

a) categories of information likely to be available

A selection of reports and materials, including selected working papers, is available to the public on the website or may be provided electronically or in paper form.

The following categories of information are accessible to members of the Religious Society of Friends in Britain with the consent of the originating department:

- Reports, minutes, and papers not marked confidential.
- Correspondence not marked confidential that does not contain personal details.
- Correspondence not marked confidential that does contain personal details where the individuals concerned have given consent for their details to be made available.

b) categories of information likely to be restricted

The following categories of information are likely to be treated as confidential by the Yearly Meeting and subjected accordingly to restrictions on access:

- Reports, minutes, papers and correspondence marked confidential.
- Correspondence containing personal details, where the other party to correspondence has not given consent.
- Correspondence between the Yearly Meeting and other bodies or individuals, except where the other party has given consent.
- Information about the financial position of partner organisations.
- Information relating to legal proceedings or law enforcement.
- Information disclosure of which could lead to improper gain or advantage or which would compromise the Yearly Meeting's position or Quaker values.
- Personnel and payroll records, except in summary statistical form.
- Medical information provided in confidence.
- Information relating to grievance and disciplinary procedures involving members of staff.
- Information about any person or any other disclosure which would constitute an unwanted invasion of privacy, a breach of the provisions on data protection or a breach of this policy.
- Information supplied in confidence by a person who has not consented to its disclosure.
- Information, opinions and assessments given in relation to recommendations for nominations.
- Information concerning disputes between individuals or in meetings or concerning appeals, for example over membership.

Britain Yearly Meeting's Data Protection Policy

1 Data Protection

The term 'data' covers information held on a computer or other automated equipment or formally organised paper records as well as data in staff personnel folders (excluding employment references), suppliers' files and customer records.

Such data is governed by the Data Protection Act 1998, which is designed to protect information processed by a computer or other automated equipment or formally organised, manually processed paper files.

The Act is concerned only with information which relates to a living individual.

The fundamental principle of the Act is that data can be kept and used only if the individual to whom the data relates is made aware of the purposes for which the data will be kept and used and (except in certain limited cases) has consented to that use.

It is important that everyone concerned is aware of the Act and abides by its rules.

2 Data held by Britain Yearly Meeting

Britain Yearly Meeting holds data on individual people, such as members, donors, suppliers, customers and staff, both on computer or other automated equipment and in formally organised manually processed paper files. We hold this information to enable us to service the Yearly Meeting and its membership, for nominations and for staff management purposes. For example we hold paper copies of general meeting and area meeting membership lists and hold these details electronically unless members have expressly asked for them to be withheld.

We also hold details of members' interests and experience for central nominations and personal details of staff and volunteers, for example addresses and names of next of kin, as part of normal personnel management.

3 Yearly Meeting data protection policy

The Yearly Meeting will meet its obligations under the Act by:

- a) Ensuring that Britain Yearly Meeting (the Data Controller) is registered with the Information Commissioner and appointing the Recording Clerk as BYM's Compliance Officer for data protection purposes.
- b) Ensuring that personal data held is
 - Obtained and used fairly and lawfully i.e. with the consent of the subject (except in certain limited cases)
 - Used only for purposes specified prior to obtaining the data
 - Adequate, relevant and not excessive.

- Accurate and kept up to date.
- Not kept any longer than necessary.
- Kept and used in accordance with the Data Protection rights of individuals.
- Protected by adequate security measures, to prevent unauthorised use, or loss or corruption, and
- Not transferred to a country outside EU without adequate protection.

c) Ensuring that members are aware of the Yearly Meeting's policy on data protection and its implications for both members and attenders.

4 Scope and implications of the Yearly Meeting's data protection policy

This policy covers members, staff and volunteers in all the constituent meetings and other bodies which constitute parts of Britain Yearly Meeting, reflecting the scope of the current BYM registration.

Our registration is restricted to official bodies of BYM and does not include non-constituent organisations, for example *The Friend*, FWCC, Woodbrooke, or listed informal Quaker groups. It does not include regional or area meetings which have registered as charities with the charity commission or any regional meetings which are no longer part of the administrative structure of BYM. These organisations should make their own arrangements for data protection registration (see [page 4](#)).

5 Responsibilities of clerks of the Yearly Meeting and constituent bodies (see item 4 above)

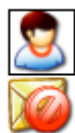
Clerks of committees and meetings covered by Britain Yearly Meeting's data registration and Directors of Friends Trusts Ltd must ensure that:

- Their members are aware of the Yearly Meeting's policy on data protection and its implications for both members and attenders.
- Data which they collect for their own use, including minutes of elders, overseers and nominations committees, as well as membership information is kept and used in accordance with this policy.
- They obtain explicit permission for the listing or processing of personal data from individuals who are not members or for details of children and young people under 18.
- The Data protection compliance form is completed annually and returned to the Recording Clerk, who is our Data Compliance Officer.

6 The Yearly Meeting's membership database

Members' and attenders' contact information is held on the Yearly Meeting's centrally-held electronic database. The database also holds all our records of donors so that everyone, whether Friend or non-Friend, who has given money to the Yearly Meeting is listed with the necessary details of Gift Aid, tax reclaimed, etc. This is a necessary part of the Yearly Meeting's accounting procedures.

Friends who do not give permission for their contact details to be held will be



recorded for contact purposes on the database by name only (Meeting for Sufferings minute 8 of 6 July 2002). These members will be identified by this icon at the top left of the database contact details window and correspondence sent via the database will automatically be blocked.

Changes in personal details held on the Yearly Meeting's membership database are made when they are received. Access to the centrally-held electronic database is password protected and staff permissions are limited by their need to use and process the information. Committee secretaries regularly update committee mailing lists. **Staff are not permitted to give out personal addresses or telephone numbers without the prior consent of those concerned.**

7 Access to data

The Yearly Meeting will allow access to its data only to those people who have a need to use it for declared purposes. Since some of the data is collected by area meetings, its processing and updating will necessarily include a regular interchange of the appropriate data with all area meetings.

The Yearly Meeting will not give out personal information on individuals to third parties, other than to comply with legal obligations (for example to police with a warrant), without the consent of the individual concerned. This applies to requests from members of other Quaker bodies, banks, building societies, prospective employers, etc.

The Act allows individuals the right to see personal data held about themselves. The procedure for access to data is outlined in the Appendix below; the Yearly Meeting will not levy a charge on individuals requesting access to their personal data.

Any Friend wishing to see the membership database, to view their own record, or to inspect the procedures for security may contact the head of communications and fundraising [*now head of communication & services*] to arrange a visit.

Requests from an individual to see personal data about themselves held only by the local meeting or area meeting can be dealt with by the AM clerk, and BYM staff at Friends House can advise if necessary.

The general rule is that personal data held on an individual may be disclosed only to that individual or with the individual's consent. Failure to observe this rule could be deemed a criminal offence and the offender may be subject to prosecution. Employees may also be subject to disciplinary action by Britain Yearly Meeting.

8 Data Control

The Recording Clerk is accountable to Britain Yearly Meeting Trustees for the registration of the Yearly Meeting's use of data to the Information Commissioner and for regular auditing of the effective operation of data control procedures for

BYM staff.

A staff data safety committee will meet at least twice yearly to oversee the implementation of this policy, prepare an annual audit report and deal with any issues arising. The report of the committee will be received by Britain Yearly Meeting Trustees.

Data Protection Policy Appendix

How to make a request to see data about yourself

If you wish to see personal data about yourself held by the Yearly Meeting you are advised to:

- Submit a 'Request for Access to Personal Data' in writing to the relevant department at Friends House describing the information you want. If you are unsure which department to write to, please write to the Data Compliance Officer.
- If you wish to see personal data about yourself held only by your local meeting or area meeting you are advised to contact the AM clerk.
- To help locate the information please give as much detail as you can about the information you would like. Your request should be reasonable; for example, you cannot ask to see every mention of you in minutes.
- You can expect the information to be provided within 40 days.
- You can either make an appointment to view the data, or copies of data held will be sent by post. If you ask to view the data you can only do so in the presence of staff or officers. Copies of your data can be provided, if you wish, but data cannot be removed from files.
- If you are unhappy with the way your request was handled or disagree with any detail contained within the file you should notify the department or AM clerk who has been dealing with your request. They will investigate the matter and inform you of the decision. If you are unhappy with the decision you may write to the Data Compliance Officer.
- If you are still unhappy, you may make a complaint to the Information Commissioner's Office. Details about complaints are available here: <http://ico.org.uk/complaints>

What to do if you receive a Request for Access to Personal Data

If you are a member of staff or officer of the Society you may receive requests from individuals to see personal data held about him/herself.

- You must provide the information within 40 days of receiving the request.
- If it is clear what personal information is being requested and you have no reservations about giving the information then do so. You can either send copies of the data, or arrange for the person making the request to view it. If they ask to view the data, they can only do so in the presence of staff or officers.

- If the request is made to the AM clerk, then you should first establish if the request is to see data held only by the local or area meeting, or by the Yearly Meeting. Anyone making a request has a right to see personal data about themselves by the Yearly Meeting. If this is what they are requesting then you should pass the request to the Data Compliance Officer at Friends House.
- If the request is to see personal data held only by the local or AM, then the AM clerk may answer it. A record of the request should be kept for compliance purposes and in case there are any queries. The annual compliance form will ask if the AM has received any requests or not.
- If you have any reservations about a request and how to handle it, then please contact the Data Compliance Officer at Friends House.

Responsibilities for protecting access to data

- If you are involved in carrying out the work of the Yearly Meeting or a local meeting you are obliged to comply with the data protection principles and should bear this in mind when recording or using personal data, setting up new systems containing personal information, changing existing systems, contemplating using data in existing systems in new ways, or disclosing it to new recipients.
- You are not permitted to use personal data for any purpose not connected with your service to the Yearly Meeting or to browse through the data out of curiosity.
- If you deal with the general public or any other external contacts such as suppliers, customers, other business contacts, government bodies, etc. you should ensure that you take great care in relation to the disclosure of personal information.
- If you use information about individuals, for example as a committee member of interview panels reviewing application forms or references, or as a member of nominations committees reviewing nominations, you should ensure that the information is returned to the personnel office or relevant committee secretary, as appropriate, after use. You should also be aware that interview and nominations notes should contain factual evidence and not personal opinions.

Appendix 2: Sample forms and examples

Example of the area meeting compliance questions

The compliance form will be sent to area meetings (which have not yet registered with the charity commission) annually by the Recording Clerk's Office. The example questions are included here for information.

Data compliance for Area Quaker Meeting:

1. Have you taken reasonable steps to ensure that all members/attenders* in the area meeting, including local meetings, are aware of the BYM data protection policy and its implications?
2. Have you obtained explicit agreement for the listing and using of personal data from individuals not in membership and from the parents or guardians of children and young people under the age of 18?
3. Are all the officers of meetings and committees who keep and use personal information on members keeping it in accordance with the BYM Data Protection and Information Security Policies?

If you have answered NO to any of the prior questions, please use this space to explain. Please also use it to let us know of any additional support from Friends House that would be useful.

(blank space for explanation removed)

- 4(a) During 20xx did anyone ask to see their personal records?
- 4(b) If **yes**, did you give access?
- 4(c) If you refused, please explain why you did not give access:

(blank space for explanation removed)

* These are attenders who are listed in your contact list and/or are active in your area meeting

Summary of Quaker Data Safety and Information Security

Quaker meetings will need to store information about their members and attenders (on computers, other devices or in paper files), they will be sensitive to the need to protect such information from unauthorised use and will comply with all legal requirements for data protection. The Data Protection Act 1998 gives protection to individuals in the holding of and disclosure of personal information. Under this legislation and in accordance with the data protection policy of Britain Yearly Meeting, we need your consent to use your personal information.

Basic factual information on members such as addresses should be kept by the area meeting on the official register of members (*Qf&p* 11.37) which should be explained to all those applying for membership. Membership information will be shared with the Yearly Meeting contact database, though members may request, by using a consent form, that information other than their name be withheld.

Information on attenders and the non-member spouses/partners of members may be held and used only with their consent. Information on children not in membership may be held and used only with the consent of their parent or guardian (*Qf&p* 11.39 and 4.45). Consent forms should enable non-members to opt for their details not to be included in published address lists or to be passed to the Yearly Meeting database or to other Quaker bodies.

Friends should be aware of the difficulty of maintaining perfect security of the lists, and they should be given the option of not publishing some or all of their personal details (*Qf&p* 4.45). If meetings record any other information on members and attenders, whether electronically or in paper-based records, for example in connection with nominations work or with applications for membership, then the persons concerned must understand that the information is held and that they may see and approve their own record. (*Qf&p* 4.45).

How your information is used, with your consent

Your details are primarily used to help members of your meeting and other constituent parts of Britain Yearly Meeting to contact one another. Information will be used for:

- Printing the address list of members and those associated with the area meeting.
- Mailing newsletters and other communications.
- Contacting you on the meetings' legitimate business.
- Pursuing the general purposes of constituent Quaker meetings.

The central offices of Britain Yearly Meeting will not use your details for unsolicited direct mail seeking financial contributions. Your information is confidential and will not be passed to other organisations without your consent.

If you have any queries please contact either the Recording Clerk (Data Compliance), Friends House, 173 Euston Road, London NW1 2BJ or your area meeting membership clerk.

Sample data consent form for a meeting

..... Quaker Meeting data consent form

Quakers seek to be clear and transparent in the work that we do and in our recording and use of your personal information. In order to nurture the life of our meetings, we would like to collect and use contact lists to administer our meeting activities at local and national levels.

We work to safeguard the information that we use and we follow Britain Yearly Meeting's Data Protection policy which complies with the Data Protection Act 1998. This form enables you to permit our use of your information within our area meeting and Quaker bodies including Britain Yearly Meeting.

We would like details of all who come regularly to our meetings and for their family members if appropriate. With your permission, we would like to share these contact details with other meetings and Quaker bodies. Your details will not be passed on to other third parties without your permission.

Young people under 18 may be included on an adult's form, however please use a separate form for each adult. Please contact if you have any questions.

Thank you. clerk to Meeting

Please use a separate form for each adult

Your name:		
Your address:		
email:		
phone number(s)		
Name(s) of children under 18:		
Details may be shared:	for printing in our local contact lists	Yes / No
	with our Yearly Meeting contact database	Yes / No*
	with other Quaker bodies	Yes / No
* (members' names are always shared with Yearly Meeting)		

I consent to the use of this information as indicated, until such time as I submit a revised form:

Signature:

Date:

Please return this form to

Appendix 3: QList – an online facility for meeting membership lists

QList is a secure web-based service set up by Britain Yearly Meeting to help local and area meetings administer their contact and membership lists. It is designed to support local and area meetings, and offers facilities for an administrator to:

- view and edit contact details, and the contact's relationship with a Quaker meeting
- view and edit the information contained in a meeting's entry in the Book of Meetings
- download information for printing or sharing
- select which information is shared, and with whom
- communicate with QList representatives at other Quaker meetings
- move QList details between meetings when individuals move.

QList contact details can be completely independent from the separate contact list system used by staff of Britain Yearly Meeting. Security has been built into QList and contact details for an individual have options which allow them to be held completely confidentially within a local meeting, until that individual is ready to begin to engage with the wider Quaker community, when the options can be changed.

If you'd like to find out more about QList please visit the webpage www.quaker.org.uk/qlist or contact Gary Mitchell via email on qlist@quaker.org.uk.