Pacific Yearly Meeting
Communications Committee

Policy Documents

in effect as of March 5, 2022

2018-07-16: Website Policy
2019-07-15: Data Breach Policy
2020-03-07: Personal Data Privacy Policy
2021-07-28: Database Policies
2022-03-05: Email Distribution List Policy
Pacific Yearly Meeting
Website Policy

This statement, approved in PYM plenary session, July 16, 2018, updates and replaces the website policy statement approved in 2007.

Purposes

The purposes of the official Pacific Yearly Meeting Website are to:
1. Support communication within Pacific Yearly Meeting (PYM),
2. Inform the PYM community, other Friends, and the world at large about relevant activities and events, and
3. Introduce the general public to Friends and to PYM-affiliated Quarterly Meetings, Monthly Meetings, and Worship Groups.

Policies

1. Website Management
   1.1. The PYM Website is under the care of the PYM Communications Committee, which is responsible for its technical maintenance, design, and content.
   1.2. Communications Committee shall appoint and define the duties of “Editors” and other roles as needed to develop and maintain the site.
   1.3. Editors are automatically ex officio members of Communications Committee if they are not otherwise already members.
   1.4. Only the Editors may actually place and remove content on the Website.
   1.5. The Editors may publish any content that serves the Purposes of the Website and is consistent with these Policies.
   1.6. In case of uncertainty about the appropriateness of content posted or proposed for the Website, the Communications Committee as a whole will discern.

2. Content Guidelines: Friends Practices and Beliefs
   2.1. The Website should reflect and serve PYM as a community and not necessarily Friends in general.
   2.2. PYM’s Faith and Practice and foundational documents (e.g., Bylaws, Articles of Incorporation, policies, etc.) should serve as a guideline for what goes on the Website.
   2.3. The Website also publishes material supporting the charges of PYM officers, staff persons, committees, or delegates; or Quarterly Meetings, local meetings or organizations within PYM.
   2.4. The Website may contain statements about Friends’ practices and beliefs, as long as any such statement reflects the viewpoint or practices of a significant number of Friends, or is an important statement about Friends, either from the past or in the present. Such statements do not necessarily have to represent an adopted position of PYM, or even the views of any Quarterly Meeting or Member or Attender of a Monthly Meeting or Worship Group in PYM. Typically, attribution is given for statements by individual Friends or identifiable groups of Friends when published on the PYM website.
   2.5. In cases where a statement might be mistakenly construed that it represents the considered opinion of PYM, when in fact it does not, an explicit notice, “This statement does not necessarily reflect the views of Pacific Yearly Meeting,” will be displayed near the statement.
2.6. From time to time, PYM might formally agree to publish a statement that does reflect a viewpoint that has been considered and approved by PYM. Such statements will be marked as such.

2.7. The Website may use links to outside organizations with which the PYM has a strong and comfortable relationship (such as organizations to which PYM makes financial contributions or sends representatives) or as the Editors determine to be in good order. On occasion, content from outside organizations may be published directly on the Website with appropriate attribution.

3. **Content Requests:**

   3.1. All requests for publication on the Website should be submitted to the Editors (in some cases via the PYM Assistant to the Clerk).

   3.2. Requests for publication of material should be made with sufficient lead time.

   3.3. The Editors may suggest changes to, or reject entirely, proposed content that, in their judgement, does not conform to the purposes and guidelines of the Website.

   3.4. Content placed on the Website should generally be attributed (name and role of the author) and dated when entered.

   3.5. It is the responsibility of the submitter to inform the Editors when content becomes obsolete and should be changed or removed; nevertheless, the Editors may remove content at any time.

4. **Privacy and Data Security**

   4.1. Communications Committee will develop a separate policy proposal covering web privacy and data security, which will go through the usual PYM seasoning process.

   4.2. We intend that the Website comply with all applicable privacy and data security regulations, such as the European Union General Data Protection Regulation (GDPR).

   4.3. We intend to reasonably protect the privacy of members of the PYM community while retaining the ability to share enough information to conduct and communicate the work of PYM.

5. **Accessibility**

   5.1. Information on the Website should be accessible to people with disabilities, conforming as much as possible with generally accepted accessibility guidelines, such as the W3C Web Content Accessibility Guidelines.

   5.2. Material should be formatted as much as possible to allow quick viewing by visitors with average computer skills.
Pacific Yearly Meeting Data Breach Policy and Plan

(Working Version)

Published: 6/11/2019  Approved: Communications Committee, 6/13/2019
Approved at Annual Session 2019-07-15, Minute AS 2019-3: Data Breach Policy

This “Policy and Plan” aims to help PYM manage Personal Data breaches effectively. PYM holds a limited amount of Personal Data about individuals who use services supported by PYM.

PYM places a high premium on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

A data breach generally refers to the unauthorized access to and retrieval of information, which may include corporate and / or Personal Data. Data breaches are generally recognized as one of the more costly security failures of organizations. They could lead to financial losses, and cause Friends to lose trust in PYM.

Scope
This policy applies to all Friends who are responsible for managing data held by PYM. Such Friends must be familiar with this policy and comply with its terms. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be approved by the PYM Communications Committee (PYM ComCom). The committee’s Data Breach Team (a subcommittee of ComCom) is charged to fulfill this policy and directly manage any data breach incident responses.

Training
All Friends who manage data held by PYM will receive training on this policy. New members of PYM committees and offices will be offered training within the first month of their new service terms. While some committees and offices such as ComCom, Ministry and Oversight, Youth Programs, Presiding Clerk, Assistant Clerk, and Registrar are likely to manage applicable data, all committees and officers will be offered training on this policy prior to accessing PYM data.

Training will be provided at least once a year and whenever there is a substantial change in the law or our policy and procedure.

Training is provided through one-on-one or small-group review of the policy and applicable laws relating to data protection.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Clerk of PYM ComCom at pym.website@gmail.com.
Personal Data
Personal Data is any information relating to an individual, whether it relates to his or her private, professional or public life. It includes such things as a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.

Any use of Personal Data is to be strictly controlled in accordance with this policy.

While some data will always relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute Personal Data unless it is associated with, or made to relate to, a particular individual. Generic information that does not relate to a particular individual may also form part of an individual’s Personal Data when combined with Personal Data or other information to enable an individual to be identified.

PYM gathers Personal Data for two purposes: for Annual Session registration and to disseminate contact information among members of the PYM community who need to contact each other. Such Personal Data may include in user profiles:

- Information such as Full name, Mailing address, Email address, and phone numbers
- Information on housing placements and support needs at annual session, such as age, allergies and mobility limitations
- Preferences for participation in aspects of annual session, such as meal preferences, and workshop preferences
- Information to facilitate payment of fees for annual session, such as family members, payment methods, and amounts paid
- User profile information to fulfill insurance or other due diligence requirements, such as results of background checks for adults working with minors in youth programs at annual session or at any other PYM events or activities.

Personal Data that PYM committees gather for internal operational purposes (such as information on job applicants or surveys of participants in PYM-sponsored events) is not stored on the PYM website, but may be stored on devices or online accounts of individual committee members.

Causes of Data Breaches
Data breaches may be caused by Friends responsible for PYM data sets, parties external to the organization, or computer system errors.

Human Error
Human Error causes include:
- Loss of computing devices (portable or otherwise), data storage devices, or paper records containing Personal Data
- Disclosing data to a wrong recipient
- Handling data in an unauthorized way (e.g., downloading a local copy of Personal Data)
• Unauthorized access or disclosure of Personal Data by volunteers or staff (e.g., sharing a login)
• Improper disposal of Personal Data (e.g., hard disk, storage media, or paper documents containing Personal Data sold or discarded before data is properly deleted)

Malicious Activities
Malicious causes include:
• Hacking incidents / Illegal access to databases containing Personal Data
• Theft of computing devices (portable or otherwise), data storage devices, or paper records containing Personal Data
• Scams that trick Friends in PYM into releasing the Personal Data of individuals

Computer System Error
Computer System Error causes include:
• Errors or bugs in applications supporting PYM’s website or other software used by PYM or Friends
• Failure of cloud services, cloud computing or cloud storage security / authentication / authorization systems

Reporting Breaches
PYM ComCom has an obligation to report actual or potential data protection compliance failures. This allows us to:
• Investigate the failure and take remedial steps if necessary
• Maintain a register of compliance failures
• Notify PYM’s Ministry and Oversight Committee of data breaches
• Notify law enforcement of any data breach failures that are material either in their own right or as part of a pattern of failures

If a data breach occurs, PYM ComCom will notify any affected individuals without undue delay after becoming aware of a Personal Data breach. However, PYM does not have to notify the data subjects if only anonymized data is breached. That is, the notice to data subjects is not required if the data affected by the data breach has been previously processed to remove any personally identifiable information.

Notifications include the following information, where available:
• Extent of the data breach
• Type and volume of Personal Data involved
• Cause or suspected cause of the breach
• Whether the breach has been rectified
• Information on how individuals affected by the data breach are being notified
• Contact details of PYM ComCom members from whom affected individuals receive further information or clarification

When specific information of a known data breach is not yet available, PYM ComCom will send an interim notification, comprising a brief description of the incident.
Data Breach Team

The Data Breach Team (DBT) is a subcommittee of PYM ComCom and shall include the Clerk of PYM ComCom.

Data Breach Management Overview

Upon being notified of a (suspected or confirmed) data breach, the Data Breach Team will immediately initiate the data breach management & response plan.

PYM ComCom’s data breach management and response plan is:

1. Confirm the Breach
2. Contain the Breach
3. Assess Risks and Impact
4. Report the Incident
5. Evaluate the Response & Recovery to Prevent Future Breaches

Confirm the Breach

The DBT will act as soon as it is aware of a data breach. When possible, it should first confirm that the data breach has occurred. It may make sense for the DBT to proceed to contain the breach on the basis of an unconfirmed reported data breach, depending on the likelihood of the severity of risk.

Contain the Breach

The DBT should consider the following measures to contain the breach, where applicable:

- Shut down the compromised system that led to the data breach.
- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach. (e.g., remotely disabling / wiping a lost notebook containing Personal Data of individuals.)
- Prevent further unauthorized access to the system.
- Reset passwords if accounts and / or passwords have been compromised.
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and/or remove external connections to the system.

Assess Risks and Impact

Knowing the risks and impact of data breaches will help PYM ComCom determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

Risk and Impact on Individuals

- How many people were affected?
A higher number may not mean a higher risk, but assessing this helps overall risk assessment.

- Whose Personal Data had been breached?
  Does the Personal Data belong to committee members, website visitors, or minors?
  Different people will face varying levels of risk as a result of a loss of Personal Data.

- What types of Personal Data were involved?
  This will help to ascertain if there are risks to reputation, identity theft, safety and/or financial loss of affected individuals.

- Any additional measures in place to minimize the impact of a data breach?
  Eg., a lost device protected by a strong password or encryption could reduce the impact of a data breach.

**Risk and Impact on organizations**

- What caused the data breach?
- Determining how the breach occurred (through theft, accident, unauthorized access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in the management of Personal Data by PYM.
- When and how often did the breach occur?
  Examining this will help PYM ComCom better understand the nature of the breach (e.g., malicious or accidental).
- Who might gain access to the compromised Personal Data?
  This will ascertain how the compromised data could be used. In particular, affected individuals must be notified if Personal Data is acquired by an unauthorized person.
- Will compromised data affect transactions with any other third parties?
  Determining this will help identify if other organizations need to be notified.

**Report the Incident**

By notifying affected individuals if their Personal Data has been breached, PYM ComCom will encourage individuals to take preventive measures to reduce the impact of the data breach, which will also help rebuild community trust in PYM and PYM ComCom.

**Whom to Notify:**

- Notify individuals whose Personal Data has been compromised.
- Notify other third parties such as banks, credit card companies or law enforcement, where relevant.
- Law enforcement should be notified if criminal activity is suspected (e.g., hacking, theft or unauthorized system access by an employee).

**When to Notify:**

- Notify affected individuals immediately if a data breach involves sensitive Personal Data so they may take the necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved or if any material new information is learned.
Notification overview:
- The Data Breach Team will reach out via email and telephone to affected individuals, taking into consideration the urgency of the situation and number of individuals affected.
- Notification will be specific, in plain language and provide clear instructions on what individuals can do to protect themselves, including:
  - How and when the data breach occurred, and the types of Personal Data involved in the data breach.
  - What PYM ComCom has done or will be doing in response to the risks brought about by the data breach.
  - Specific facts on the data breach, where applicable, and actions individuals can take to prevent that data from being misused or abused.
  - Contact details and how affected individuals can reach members of the DBT and PYM ComCom for further information or assistance (e.g., phone numbers, e-mail addresses, webpage links).

Evaluate the Response and Recovery to Prevent Further Breaches
After steps have been taken to resolve the data breach, PYM ComCom will review the cause(s) of the breach and evaluate whether existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring again. Wherever possible, PYM ComCom will put a stop to practices that led to the data breach. This will encompass operational and policy-related issues, resource concerns and issues concerning the internal procedures of PYM ComCom.

A brief report on any data breach incident and the correct actions taken by PYM ComCom will be posted on our website. A full post-incident analysis will be made available to anyone who requests it.

Monitoring
- All Pacific Yearly Meeting committee and staff members and volunteers with access to PII data on PYM members must observe this policy.
- PYM ComCom has overall responsibility for this policy.
- PYM ComCom will review and monitor this policy in response to changes in technology, regulatory or legal changes or new concerns or data breach incidents.
Pacific Yearly Meeting Personal Data Privacy Policy

Published: 6/11/2019  
Approved: 7/15/2019 (Version 4.2)  
Revised: 2/12/2020 (Version 4.3)  
Approved: March 7, 2020 (Version 4.3)

Overview
This policy pertains primarily to the website of Pacific Yearly Meeting of the Religious Society of Friends. You can read more about Pacific Yearly Meeting here, and our main website is http://www.pacificyearlymeeting.org. As of the publication date, this is the current working policy of the Communications Committee. It was approved by Pacific Yearly Meeting at Annual Session 2019.

What Personal Data we collect, and why we collect it
Personal data collection principally occurs and is managed through the website and the PYM directory database. Personal data that is extracted from the website, such as event registration records, are also governed by this policy.

Comments
When you leave comments on the PYM website, we collect the data shown in the comments form, and also your IP address and browser user agent string to help with spam detection.

Media
We try to avoid uploading location data (EXIF / GPS) that might be embedded in images published on our website. We encourage visitors to avoid this as well. Such location data can be extracted by other website visitors, which might be against the wishes of the people depicted in the images.

Documents
Documents and other website content with personally identifiable information (PII) -- like email addresses, street addresses, and phone numbers -- should be explicitly approved for posting on the website by anyone with PII reflected in those documents. PII in website content presents an exposure of this information to anyone visiting our website (manually or programmatically).

Contact forms
We have various contact forms throughout the website. In addition to sending an email to the appropriate contact person for the information you have submitted, the submitted information will be stored, along with your IP address (references the device from which the form was submitted) and browser user agent string to help with spam detection.

Cookies
This site uses cookies as a default capability of our platform (WordPress). Cookies are small files placed
on the user’s computer. Among other things, these allow us to see the IP addresses of visitors and give us information about who is using the website. These cookies can be removed manually by the user using standard browser functions.

When you log in, we may set up cookies to save your login information and your screen display choices. Login cookies last for two days, and screen options cookies last for a year. If you select "Remember Me", your login will persist for two weeks. If you log out of your account, the login cookies will be removed.

If you edit or publish an article on the website, an additional cookie will be saved in your browser. This cookie includes no Personal Data and simply indicates the post ID of the article. It expires after 1 day.

Embedded content from other websites

Articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if you had visited the other website. These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content.

Pacific Yearly Meeting does not collect usage or other information about user interaction with those third-party sites.

Registration for Yearly Meeting programs and events

The website houses the registration system for the Annual Session of Pacific Yearly Meeting. These data are retained throughout the registration and post-registration period to aid the committees of the Yearly Meeting involved in planning, coordinating and evaluating the Annual Session. This information includes Personal Data like names, home and email addresses, and phone numbers entered by registrants. Access to this data is restricted to select people directly involved in coordinating the Annual Session event and limited to the information required for each purpose. These select people include the Registrar, members of the Arrangements and Ministry and Oversight committees, the Statistical Clerk, the appointed technical individual(s) who support the site and other individuals delegated by the yearly meeting to coordinate youth programs.

Registration data is also used to produce the Annual Session attenders list, which is printed and distributed to program participants and PYM committee members. There will also be an option to exclude specific people from this listing, upon request.

Membership data and online directory

The Yearly Meeting has plans to implement an online directory, which would house all of the relevant information found in monthly and quarterly meeting directories, plus information on yearly meeting committee members, officers, representatives and liaisons. Data within the directory will be restricted for access by authorized users. Authorized users for each monthly meeting would have access to all of the directory information for their own meeting, plus more limited information on the Quarterly and Yearly meeting clerks, committees and so on. Authorized monthly, quarterly and yearly meeting delegates would be able to maintain and distribute directory information for their respective constituencies.
The data gathered and managed for the PYM directory will be used for publishing the directory, and individual contact information in the directory will only be shared with approved recipients within PYM and its affiliated organizations. Additionally, information within the directory system may be used for communications, including email, phone calls or correspondence by Yearly, Quarterly and Monthly Meeting committees and officers in carrying out their service in their respective roles.

**How we protect Personal Data**
We maintain appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your Personal Data, including usernames, passwords, transaction information and other data stored on our sites. We will delete or de-identify your online Personal Data when it is no longer needed for its original stated purpose.

**Your privacy rights**
As an individual you may:

- Ask us to provide you with information regarding the Personal Data housed on the site pertaining specifically to you.
- Provide information to rectify, update or complement inaccurate or incomplete Personal Data concerning you.
- Request that we delete all online Personal Data identifiably pertaining specifically to you.
- Notify the Pacific Yearly Meeting Clerk or Ministry and Oversight Committee if you are unhappy with the way we have treated your Personal Data or any related privacy request you have made of us (see https://www.pacificyearlymeeting.org/contact-us/).

**Analytics**
In order to better serve the users of our site, we use analytics software to see what browsers, operating systems, and devices our users are logging in with. Analytics also track geographical location of users; however, your specific IP address is anonymized so your personal location is not tracked.

**Who we share your data with**
We do not share any information about our site visitors with outside non-affiliated organizations. All information collected is explicitly for the use of Pacific Yearly Meeting and its constituent Quarterly Meetings, Monthly Meetings, and Worship Groups, as well as Quaker organizations formally affiliated with PYM when this includes an approved sharing of PYM directory information.

**How long we retain your data**
We do our best to maintain accurate records of all our site activity. Most of this information is retained indefinitely. However, registration information collected via forms or surveys is retained up to three years online, then only retained offline as needed for PYM planning purposes.

Currently we do not offer commenting or discussion on our sites. Should we enable this capability in the future, it will offer standard WordPress functionality: If you leave a comment, the comment and its metadata will be retained indefinitely. This will allow us to maintain a history of any public conversations among PYM Friends that occur on the PYM website. For users who register on our website, we also indefinitely store personal information provided in their user profiles. All logged-in
users can see, edit, or delete their personal information at any time (except they cannot change their username). Website administrators can also see and edit that information.

**What rights you have over your data**

If you have an account on this site, or have left comments, you can request to receive an exported file of the Personal Data we hold about you, including any data you have provided to us. You can also request that we erase any Personal Data we hold about you, and we will do our best to erase it. However, we will not erase any data we are obliged to keep for legal or security purposes or for necessary administrative functions like financial record-keeping. We collect registration and survey information through our site. This data is not shared publicly online, though aggregated summaries of such data may be shared. We will remove any records with your personal information from our website, if you request in writing that we do so. This information may be retained offline indefinitely for planning and administrative purposes.

**Where we send your data**

All data we collect is explicitly for use by Pacific Yearly Meeting and its constituent members, meetings, worship groups, quarterly meetings and affiliated organizations. We do not share any information about our site visitors with outside and non-affiliated organizations.

Visitor comments may be checked through an automated spam detection service.

**Your contact information**

Visitors submitting comments or creating user accounts on our site will share their IP and email addresses with us. Access to IP and email addresses submitted in this way is restricted to site administrators.

Contact information submitted through registration and survey forms is only used internally by our planning committees and is not shared online or publicly.

In the future, personal information may be included in an online member directory, available only to members of PYM. Contact information will be excluded or removed from this directory if you request in writing that we exclude it.

**Additional information**

**How we protect your data**

The PYM Communications Committee and web hosting providers do their best to protect our online resources from malicious usage or unauthorized intrusion. Our hosting company follows best accepted security procedures, and we do our best to keep abreast of current security concerns and to install defenses against hackers, spam, and other efforts to compromise our site(s).

**Data breach procedures we have in place**

If we discover that our site(s) or data have been compromised, we will notify all potentially affected users of the site immediately by email of that attack. We will also publicly notify site visitors of the
situation through a post on the site(s) within a week of the discovery of any data breach. Please review our [Data Breach Policy](#) for more details.

**Third parties we receive data from**

We do not collect or utilize data from outside organizations on our site(s), except anonymous analytics data. As a courtesy, we offer links to other sites (mainly Quaker organizations), though no data is exchanged with those sites.

**Automated decision making and/or profiling**

We do not utilize any automated decision making or advertisement suggestion software.
Pacific Yearly Meeting
Communications and Membership Database Policies

These policies were approved at PacYM Annual Session on July 28, 2021:
Minute AS 2021-09: Policies for Communications and Membership Database

Pacific Yearly Meeting Communications and Membership Database Policies

1. Information Included in the Communications and Membership Database

The PacYM Communications Committee, which is responsible for the PacYM communications database, is committed both to simplicity and to providing PacYM officers, committees, and representatives with the information they need to carry out their ministry. As of February 2021, the committee has discerned that the database will store the following information:

- full name*
- year of birth
- pronouns
- racial/ethnic identities
- mailing address
- phone number
- email address
- primary monthly meeting or worship group*
- membership status*
- roles served in primary monthly meeting
- “do not publish” option (whether the Friend’s information may be included in directories produced from the database)
- “do not contact” options (whether this Friend may be contacted by phone and/or email)
- roles served in yearly meeting and quarterly meeting (this information is provided directly by the yearly and quarterly meetings)

*designated as required fields

The committee will request that Friends with children (under 18) in their care provide the following information for each child:

- full name
- month and year of birth
- primary monthly meeting or worship group
- name of parent/guardian

Additionally, the committee will request that Friends who sometimes bring children who are not usually in their care (e.g., grandchildren, children of another Friend) to Quaker gatherings indicate this.

2. Membership Information

Communications Committee believes that for the database to fulfill its membership function, all members would need to have their names and monthly meetings recorded in the database. This information is already maintained by the yearly meeting, but in a less secure form than the database. When someone who is a member of a monthly meeting in Pacific Yearly Meeting does not provide their information for the database, the Communications Committee and Statistical Clerk, guided by the discernment of the directory manager of the Friend’s monthly meeting, may enter
into the database limited information about them from other sources (e.g., monthly meeting directories):

- full name
- primary monthly meeting
- membership status

This information will be classified as "Do Not Publish" in the database, meaning that it will not be visible in any directories generated from the database and only individuals with direct access to the database (a small number of Friends who serve in certain yearly meeting roles and who have undergone training to use the database) will be able to see and use the individual’s information. In particular, it will not be accessible through searching the internet.

3. **Access to and Transmission of Directories Derived from the Database**

Direct access to the database will be limited to as few Friends as feasible, and these Friends will be required to undergo training in how to use the database before being given access.

Any member or attender of a monthly meeting or worship group within Pacific Yearly Meeting, and any Friend serving on a Pacific Yearly Meeting committee, may view and download the current PacYM directory as a pdf from a password-protected section of the website. The pdf will also be password protected.

Friends are expected to practice respectful stewardship of other Friends’ personal information. Accordingly, Friends may not send directories by email. A Friend who wishes to share a directory with another Friend within Pacific Yearly Meeting may:

- instruct them how to download a copy from the PacYM website, or
- print a copy and share it in person or by postal mail

Friends should not share directories outside of PacYM. If someone outside PacYM needs access to a directory, they should contact the Communications Committee (communicationsclerk@pacificyearlymeeting.org).

Quaker organizations, Friends from other yearly meetings, and individuals with a need to contact Quakers (e.g., a researcher of Quaker history) may contact the Communications Committee to request directories. Communications Committee will then discern whether the request is in accordance with the policies and agreements it has made with Friends and respects the privacy needs of each person whose information is published in the directory. Data will not be shared for commercial purposes.
This policy was approved at Representative Committee meeting on March 5, 2022: Minute RC 2022-03: Policy for Email Lists

Policy on Email Lists

Definitions

An email list is a technology that allows a person to send an email message to many email addresses at once by sending it to a single group address. For example, if we had personal email addresses for Margaret Fell, the Public Universal Friend, and Bayard Rustin (e.g., margaretfell@gmail.com, puf@aol.com, bayardr@earthlink.net), we could add these personal email addresses to an email list with the address examplelist@pacificyearlymeeting.org so that someone could send a message to all three of these Friends simply by sending an email to examplelist@pacificyearlymeeting.org.

There are two types of email lists: **announcement lists**, which allow one-way communication of information, and **discussion lists**, which allow back-and-forth conversation.

Email lists in Pacific Yearly Meeting

The Pacific Yearly Meeting (PacYM) Communications Committee will create and maintain email lists using information from the PacYM communications and membership database. These lists are intended to strengthen our community by enabling Friends with similar ministries to communicate with each other and by helping PacYM officers and committees to share important information with the yearly meeting body.

Only appropriate PacYM officers, committee clerks, and PacYM employees can send emails to **announcement lists**, using their official PacYM role-based emails. PacYM Friends will be included in these lists on an opt-out basis; everyone who has an email address listed in the communications and membership database and has consented to receive emails pertaining to the yearly meeting will be automatically put on relevant announcement lists, with the option to unsubscribe given at the bottom of each message. Examples of announcement lists include:

- A list of clerks, co-clerks, and clerking teams of monthly meetings
- A list of monthly meeting representatives to Pacific Yearly Meeting
- A list of parents with children under 18 and other Friends who sometimes accompany children under 18 to PacYM events

**Discussion lists** allow anyone who is on the list to send emails to the list. Friends will be included in these lists on an **opt-in** basis; an appropriate PacYM officer, committee clerk, or employee will send an invitation to Friends identified in the communications and membership database (or otherwise self-identified) as potentially having an interest in participating. Those that do choose to join will then be added to the list, with the option to unsubscribe given at the bottom of each email if they change their mind. Examples of discussion lists include:

- A list of Friends leading children’s education or first day school at their monthly meetings
Pacific Yearly Meeting
Email Distribution List Policy

• A list of Friends leading peace and social order ministries at their monthly meetings

Friends are asked to “clerk themselves” when composing emails to discussion lists, caring for the community by considering whether the content is kind, necessary, true, and relevant to the particular list. Guidelines for use of discussion lists may evolve as we gain experience with them.

Communications Committee will receive requests from PacYM officers, committee clerks and employees and discern with the person making the request whether an email list is appropriate. Communications Committee will create new lists as needs arise, being mindful of whether proposed lists are relevant to the yearly meeting, expected to remain relevant long enough to justify their creation, and within the committee’s energy to create and maintain. Communications Committee will also lay down or merge lists as needs change.