Protected Information and Privacy Policy

Policy Definition: *a Policy is a statement that outlines the Board's intentions to live out our UU values; comply with mandates; set boundaries on actions, decisions, or activities; and delegate responsibilities. Delete this definition from the approved version of the policy.*

Intent

The Board of Trustees intends to protect the privacy of its members, friends, and staff, which includes the ethical handling of contact information, pledge history, and other sensitive information. The Board will follow all relevant law in the pursuit of this intent.

Relevant Mandates

The UUCC Board of Trustees intends to comply with relevant law in the handling of sensitive information about or from members, friends, and staff.

Boundaries

The UUCC respects and strives to maintain the privacy of its members, friends, and staff. At minimum, "privacy" is equivalent to "protected information" (PI) and includes:

- Personal Information: includes social security, credit card, or bank account numbers of individuals, and health data.
- Confidential information: includes anything a reasonable person would recognize as sensitive or potentially damaging.
- Information about minor children: including routine contact information, pictures, etc

In such cases where privacy may not be ensured, those communicating on behalf of the UUCC shall inform potentially affected parties that their communications are public and that privacy should not be expected.

The UUCC and its members and staff will not share or sell member contact information or other PI to outside parties at any time for any use. Such information may be shared internally for relevant congregational business, as deemed appropriate by the board, Leadership Council, or by committees which require this information to perform their duties.

Responsibilities

Members and staff with access to personal information shall undergo training at the beginning of each congregational year as part of the first meeting of the relevant group or committee handling the information, in order to ensure boundaries and responsibilities for the safe handling of PI and other sensitive information are met. This training shall be

developed and reviewed annually to ensure necessary updates are made to accommodate changes in technology.

The UUCC Protected Information and Privacy Policy itself shall be reviewed and amended as necessary every three years, beginning three years from date of approval.

Action Record:
Policy adopted by the Board of Trustees on November 24, 2020.

Procedures:

The following data security measures are recommended by the UUA and are provided here for consideration of the group responsible for the training regarding proper handling of information:

- Only trusted and authorized persons shall have access to protected information.
- Required use of a strong password to access computers or online data storage systems. A strong password is at least 12 characters long and includes upper and lowercase letters and digits. (That's almost a million trillion possible combinations.) It does not include names, dictionary words, birthdays, or obvious sequences of numbers. Recent research shows that the best protection comes from a long password that conforms to the rules above.
- Passwords shall be changed at least every 6 months.
- Passwords shall be changed whenever anyone loses their authority to access a computer or online data management system.
- Computers shall be set to lock automatically if not used for 10 minutes.
- Protected Information shall never be sent in an email or an email attachment.
- Laptops should be kept in a locked cabinet, or secured with a locking cable.
- All computers used to store or access protected information shall have virus detection software installed and automatically updated every day the computer is used. See "Resources" for suggestions.
- All software on computers used to store or access protected information shall be kept up-to-date, especially security updates. This includes anti-virus software, pdf reader and media players as well as Windows or Apple software.
- Firewalls shall never be disabled on computers used to store or access protected information.
- Passwords for networking equipment (e.g., cable modems, wireless routers), shall be changed when installed, including both the default administrator and network access passwords on each piece of equipment.
- Passwords to computers, network equipment, software, files, and online accounts shall be stored in an encrypted and password-protected database. Passwords shall not be written on paper or post-its, or sent in emails.