Intellectual Property, Information & Records Policies & Procedures
Rev. Anthony David

Policy

Our policy at UUCA around intellectual property, information and records is (1) to ensure that storage, maintenance and security are all effective; (2) to abide by intellectual property laws; (3) to guarantee the confidentiality of sensitive information.

Procedures

I. To ensure effective storage, maintenance, and security:

Technology Use (from *UUCA Personnel Manual*)

Overview

UUCA is committed to protecting its employees and the congregation from illegal or damaging actions by individuals either knowingly or unknowingly. This Acceptable Use Policy is not intended to impose restrictions that are contrary to UUCA's established culture of openness, trust, and integrity, but rather to protect and secure the congregation's information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly. The purpose of this policy is to outline the acceptable use of information systems at UUCA. Inappropriate use exposes UUCA to risks from virus attacks, compromises network systems and services, and compromises the integrity and confidentiality of data. This policy applies to employees, faculty, contractors, consultants, volunteers, and other workers at UUCA, including all personnel affiliated with third parties. This policy applies to the UUCA Information System which includes, but is not limited to: computers, printers, network devices, wireless access points, software, storage media, data, email, telephones, and all other equipment owned or leased by UUCA.

A. General Use and Ownership

1. UUCA's computer systems, and all data residing on those systems, are and shall remain the property of UUCA and are subject to being monitored and/or disclosed at any time by UUCA.
2. Computer use is a privilege, not a right. Use of UUCA's computers, networks, and Internet services must comply with the acceptable use guidelines outlined below.
3. Business Use: Workstations and network systems are intended for business use only. Desktop workstations are not to be used for games or for personal projects.
4. Data Ownership: Data created on UUCA's systems remains the property of UUCA. This includes all paper and digitized documents generated in the course of doing business; this material is not to be removed from the premises without authorization.
5. Employee-owned Laptops: Employees using privately owned laptop workstations are responsible for their security and are subject to all the guidelines of this

policy as appropriate. If the laptop is no longer used as a desktop workstation in the office OR upon termination of employment, all business-related data must be removed from the laptop.

B. Security and Proprietary Information

1. All employees will read and comply with UUCA's Password Policy (see below).
2. All PCs that are connected to UUCA's Information System, whether owned by the employee or UUCA shall be continually executing approved virus-scanning software with a current virus definitions database.
3. Employees are discouraged from accepting/using floppy disks and/or opening email sent from unknown or suspicious sources.

C. No Right to Privacy

Any computer files or email messages maintained, stored, received, or transmitted on or from UUCA's computer systems are and shall remain property of UUCA and are subject to being monitored and/or disclosed at any time by UUCA.

(a) have no privacy interests in email messages or passwords
(b) are deemed to consent to UUCA's monitoring and disclosure of email messages
(c) will make no claim against UUCA for monitoring email, for disclosing email, or for any other issues relative to UUCA's email system.

D. General Restrictions on Content of Email Messages

Postings by employees from a UUCA owned email address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UUCA; newsgroup browsing and posting should only be for business purposes. Employees will use extreme caution when opening email attachments received from unknown senders, which may contain viruses.

The email system has been installed by UUCA for use in the conduct of its business. UUCA recognizes, however, that employees may desire to use the email system occasionally for personal purposes. UUCA will permit such occasional, personal use of the email system, provided that:

1. Such use does not result in additional costs to UUCA;
2. Such use is not excessive or abused by employees; and
3. Employees understand (and are hereby informed) that *all* messages transmitted or received on the email system, of whatever nature, remain fully subject to all of the provisions of this email policy. Thus, even personal messages on the email system constitute UUCA's property in which employees have no right of privacy and which may be stored, monitored, or disclosed at any time by UUCA.

The email system shall not be used to transmit messages, either within UUCA or in communications transmitted outside UUCA, that might reflect poorly on UUCA, including language or material of a sexual or otherwise inappropriate nature, or that may be construed as harassment or disparagement of others based upon their race, color, national origin, sex, gender identity, sexual orientation, age, marital or familial status, physical or mental disability, religious or political beliefs, or any other characteristic of people protected by federal or state law.

The email system shall not be used for sending information outside of UUCA that constitutes the confidential or proprietary information of UUCA (except with the express permission of UUCA), nor for the unauthorized receipt of the confidential or proprietary information of others. Employees shall promptly notify the Business Manager in the event an email transmission containing the confidential or proprietary information of another party is received without the express permission of that party.

E. Physical Protection of Desktop Workstations

It is the responsibility of the person assigned to the workstation to protect the hardware and accessories from any and all damage of any kind and from use by guests or other unauthorized persons.

1. Do not move or disassemble the workstation in any way without permission from the Business Manager.
2. Provide a clean, safe, and consistent environment for all hardware and media. Workstations and accessories will be kept free from food, drinks, and magnets.
3. Cables and cords will be kept away from heaters and foot traffic damage.
4. Desktop workstations in employee offices are not to be used by guests or any authorized persons for internet access or other personal or non-business use.
5. Workstations should be logged off the network but left on when the employee leaves for the day (monitors should be turned off).
6. Workstations will be locked by screen saver when the computer is unattended for an extended period of time.

F. Document Storage

Save all documents on the “H” drive and not on the desktop or “C” drive.

G. Unacceptable Use

Use of computers, networks, and internet services of UUCA to engage in any activity that is illegal under local, state, federal, or international law or that violates UUCA’s Policies and Procedures and/or UUCA’s End Statements including procuring or transmitting material that is in violation of UUCA’s Harassment Policy is prohibited.

The following activities are strictly prohibited, with no exceptions:

1. The installation or distribution of “pirated”, downloaded or other software products that are not appropriately licensed for use by UUCA.
2. Unauthorized copying of copyrighted or patented material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation or distribution of any copyrighted software for which UUCA or the end user does not have an active license.
3. Accessing, submitting, posting, publishing, forwarding, downloading, scanning, or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, and/or illegal.
4. Installing, uninstalling, or altering software resident on UUCA’s workstations.

5. Introduction of malicious programs into the network or server (e.g. viruses, worms, etc.).
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
7. Circumventing user authentication or security of a PC, network, or account.
8. Providing information about, or lists of, UUCA employees or members to parties outside of UUCA without prior management approval.
9. Copying and disbursing UUCA information, data, databases – this includes distributing mail lists and/or databases to affiliated organizations of UUCA without prior approval.
10. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
11. Creating or forwarding "chain letters", "Ponzi", or other get-rich-quick "pyramid" schemes of any type.
12. Posting the same or similar non-business-related messages to large numbers.

Employees found to have violated the guidelines of this policy may be subject to disciplinary action.

H. Information Systems Password Policy

1. Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of UUCA's entire network. As such, all UUCA employees (including volunteers, counselors, and interns with access to UUCA's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure passwords.
Passwords covered by this policy include: user level accounts, web accounts, email accounts, and screen saver protection. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at UUCA, has access to the UUCA network, or stores any non-public UUCA information.

2. General Policy

- All user-level passwords must be changed every three months (January 1, April 1, July 1, and October 1).
- Passwords must not be given or shared with anyone within or outside the organization except the IT Consultant or the Business Manager. The one exception is the volunteer password, which can be given out as needed.
- Screen savers must be turned on; the "password protected" option on the Screen Saver setup dialog box must be checked. Screen savers must be configured to activate within thirty minutes of inactivity.
- Users are not permitted to use the same few passwords over and over again; users cannot use the same password more than once a year

- Network accounts will be locked after five unsuccessful logon attempts within 60 minutes. (Lockout means users cannot try to logon to the same account again for 60 minutes.)

3. Guidelines – All passwords must conform to these guidelines

Passwords are made up of various characters, which can be broken down into four character groups. These are:

1. Uppercase alphabetic	ABCDE…
2. Lowercase alphabetic	abcde…
3. Numeric	12345…
4. Special characters	!@#$%…

User passwords must consist of 8 or more characters and must use characters from 3 of these 4 groups.

4. Password Protection Standards

- Passwords should never be stored online.
- Do not share your password with anyone!
- Do not use the same password for UUCA accounts as for other non-UUCA access (e.g. personal ISP account, option trading, benefits, etc.).
- Do not use the "Remember Password" feature of applications (e.g. Windows, Eudora, Outlook, Netscape Messenger).
- List of don'ts:
    - Don't reveal a password over the phone to ANYONE
    - Don't reveal a password in an email message
    - Don't talk about a password in front of others
    - Don't hint at the format of a password (e.g. "my family name")
    - Don't reveal a password on questionnaires or security forms
    - Don't share a password with family members
    - Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them contact the Business Manager. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices without encryption).

If an account or password is suspected to have been compromised, report the incident to the Business Manager and change all passwords."
The IT consultant, Executive Director and Administrator are the only staff to have access to the Administrative Password for the Computer Network.

Storage of Information and Records in Paper Form

- Personnel Files and volunteer background check forms are stored in a locked office and locked cabinet.
- Financial deposit records (include copies of checks) are stored in a locked cabinet in a locked office.

- Contracts, Insurance Policies, etc. are stored in a locked cabinet in a locked office.
- If any of these records are no longer needed, they are shredded before disposing of them.

II. To abide by intellectual property laws:

With regard to the products of the ministers: The ministers' contracts include the paragraph, "All notes, research, sermons, and other products of the minister's work shall be the sole property of the minister."

With regard to performing music: There is a religious service exemption in the Copyright Law. Thus, churches are free to perform any music they want during the course of a service without having to obtain a license (i.e. permission) or paying a performance royalty or license fee.

With regard to the use of videos in worship, in religious education, and in other congregation-related contexts: We secure permission by paying an annual fee for a CVLI Church Video License. See http://www.cvli.com/ for more information. "Through an agreement with studios and producers, the CVLI Church Video License provides legal coverage for churches and for other ministry organizations to show DVDs and videocassettes of motion pictures. (Each organization needs to be specifically covered.) Coverage includes playing just a few minutes of a movie all the way up to showing the full-length feature. The Church Video License is one of the most cost effective and convenient ways for churches and other ministry organizations to protect themselves from the possibility of being fined for illegal use of DVDs and videocassettes."

With regard to the use of materials on our website, on our Facebook page, and other sites overseen by our volunteer social media coordinator: We only use pictures e-mailed directly to him. We do not use U-Tube or web-based photos or videos. Tumblr-only pictures are taken by social media coordinator or are free stock photos.

III. To guarantee the confidentiality of sensitive information

Regarding confidentiality of administrative-related information: Most of this is covered under the "Technology Use (from *UUCA Personnel Manual*)" protocol, included above. One area not mentioned is related to pledge data. This information is shared only on a need-to-know basis with Executive Team members and key Annual Campaign volunteers.

Regarding pastoral care confidentiality:

> Current Policy
> "The Pastoral Care Coordinator maintains a confidential log of pastoral care cases that is maintained in a locked file or password protected computer. The log generally identifes the date the case was opened and the actions and follow-up taken. The purpose of the log is to help Rev. Keller and the Coordinator to keep track of care given and identify need for follow-up. When a pastoral care file is officially closed, any related personal information is purged from the file. In addition all deaths are recorded on a one year

calendar system so that congregants may be contacted on the one month, six month and annual anniversary of the death. After one year the item is removed from the calendar."

Current Practice

At this time, the Pastoral Care Coordinator, Rev. Tessie Mandeville, maintains a confidential hand-written file of pastoral care cases. She logs the name, date, and situation into the log. When the lay minister (or other Minister or Coordinator) attends to the issue, the follow-up is logged in the hand-written file, along with notes for continued follow-up if applicable. The hand-written log is in Rev. Mandeville's possession at all times and is locked in a cabinet when not in use. The Coordinator files logs quarterly in a locked cabinet and shreds them annually. Records are kept this long to ensure continuity of care and to provide a living document of the ministry
being provided by UUCA.

Revs. Keller and Mandeville maintain confidential voice mails via their phones so that anyone calling with a pastoral care situation is assured of confidentiality.

Information about pastoral care situations are relayed by Rev. Keller to the Coordinator via email, in person, and via the phone. The Coordinator relays the pastoral care situation to the lay minister who is on-call that week via email, in person, and via the phone. We recognize that email communication is not private and we work with this limitation in the following ways:

1. The Coordinator sends only the on-call lay minister the email. No other person is carbon copied (cc) or blind carbon copied (bcc).

2. The Coordinator keeps an online copy of every correspondence sent and received regarding pastoral care.

3. The on-call lay minister does not forward the email to anyone else.

Future Practice

1. Recognizing that email is not private we intend to set up a private Google group in order to ensure absolute confidentiality.

2. If we cannot ensure total privacy, we will revert to contacting the lay minister by phone or in person only.