PEACE LIBRARY SYSTEM		INTERNET AND ELECTRONIC MAIL ACCEPTABLE USE	
CATEGORY:	Management and Operations	POLICY:	M4-17
DATE APPROVED:	November 25, 2017	REVIEW IN:	2022

The appropriate use of computer technology can result in more efficient and effective operations. Employees are encouraged to make use of the technologies available at the System for the purpose of conducting System business in an efficient, ethical, and legal manner.

This policy describes the terms and conditions under which Peace Library System's electronic mail (e-mail) and Internet services may be used by Peace Library System staff.

ACCEPTABLE USE (GENERAL)

The use of System hardware, software, and the Internet for illegal purposes is strictly prohibited.

During work hours, staff members may search the Internet for information relevant to their job tasks, may send relevant job-related e-mail messages, and may use other Internet programs for work-related purposes.

The System understands the benefits derived from employees who are skilled in the use of computer technologies and the Internet. To this end, staff members are permitted to use the System's computer resources before or after their work day for private purposes. However, employees are still required to comply with all acceptable use guidelines (ie. downloading, legal use of machines, etc.)

An employee who repeatedly causes hardware or software problems that require assistance from the IT Services Department, or who does not comply with Acceptable Use guidelines while using the computers for private purposes, will lose this privilege.

Violations of Acceptable Use may result in immediate disciplinary action up to and including termination of employment.

GENERAL RESPONSIBILITIES

The basic setup of e-mail and Internet programs may not be reconfigured except with prior approval by the IT Services Department. This does not include the creation of bookmarks, nicknames, or mailboxes -- these may be changed and created at a staff member's discretion.

Staff members are responsible for regularly cleaning out their e-mail, Internet temporary files and other files stored on the network drives.

Staff members are not permitted to install any software without the prior approval of the IT Services Department.

The System has taken measures to prevent viruses from being loaded onto the computer system. Staff members are required to comply with all preventative measures.

The System has also taken measures to keep the computer system secure from the outside world and hackers. Passwords and logins are to be kept confidential and users will be prompted by the system to change their passwords quarterly. Passwords should not be easy to guess and should not be a word found in an English dictionary. Passwords should be a minimum of seven characters and must include numbers and letters, at least one of which must be a capital.

The IT Services Manager will ensure an up to date password file is available and saved in a file accessible by the Director, the Executive Assistant, and the IT Department.

Information about the computer system is not to be given to outside sources other than representatives of companies that do business with the System and then only if the information is required to make a computer application work. If there are concerns or questions about providing this information, employees should consult the IT Services Manager or the Director.

INTERNET USAGE

Responsibility for Downloading Files

Staff members may download only work-related files and are expected to clean out any outdated or unnecessary files every six months.

Acceptable Use

Using the Internet for the following purposes is strictly prohibited:

1. Carrying on any commercial activity not directly related to System activities;

2. Transmission of any material covered by copyright or license without the explicit permission of the owner of the copyright or license.

ELECTRONIC MAIL

The purpose of electronic mail is to enhance communication between System staff and their colleagues, both internal and external to the organization. E-mail provides an efficient means of transmitting written messages and information.

Access to Electronic Mail Accounts

All staff members have an electronic mail account. This account should only be used for messages between specific individuals inside and outside the System. Membership on electronic list services (list-servs) is only permitted if the list-serv is work-related.

Personal use of e-mail is permitted provided that such use does not occur on System time or violate the Acceptable Use policy stated below.

Responsibility for Messages

Staff members are provided with an individual e-mail address and are responsible for all electronic mail originating from his or her account.

With the exception of the incoming general accounts, e-mail accounts may not be shared.

Acceptable Use

E-mail is a form of written communication that requires the same professionalism and respect for others required by more traditional written business communication.

Using e-mail for the following purposes is strictly prohibited:

1. The posting of messages that contain language or images which may be construed as harassing or disparaging of others;

2. Carrying on any commercial activity not directly related to System activities;

3. Posting of inappropriate messages to multiple recipients for any non-System purpose;

4. Posting or forwarding any form of "chain" letter or message;

5. Transmission of any material covered by copyright or license without the explicit permission of the owner of the copyright or licence;

6. Attempting to read, delete, copy or modify the electronic mail of others.

Non-work related attachments received as personal e-mails may not be stored on shared network directories ("P" and "X" drives).
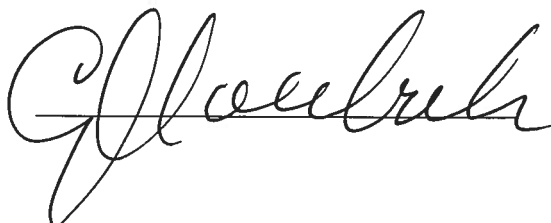
Privacy of Electronic Mail

Staff members acknowledge that e-mail messages sent to others can be forwarded to third parties, printed or inadvertently routed to individuals other than the intended recipient.

Staff members should never send or store confidential information in the e-mail system and should exercise care in reading and responding to e-mail.

System administrators will treat e-mail file contents as private information, reserving the right to inspect e-mail only to ensure compliance with this policy and to track returned (bounced) and repeatedly sent e-mail for the protection of the computer system.

Chair's Signature: