



Clinton-Essex-Franklin Library System

Use of Communication, Internet and Computer Systems Policy

*Adopted by the Board of Trustees
November 23, 2015*

Computers, e-mail and the Internet, telephones, and other computing and communications systems and devices are tools that the Clinton-Essex-Franklin Library System uses to support research and education and to provide work-related resources for its employees. Staff members are expected to use communication and computer systems in ways that advance CEFLS's interests and enhance the staff member's job performance.

Privacy:

Staff members have no personal privacy right in any material created, received, saved or sent using CEFLS's communications and computer resources. All documents and information created, received, or sent on such equipment and systems are the property of CEFLS. Limited personal use is permitted with the understanding that CEFLS reserves the right to access and review all information at any time. Therefore, employees shall have no expectation of privacy in using Internet access, e-mail, voice mail, or any other communication and computer equipment.

Passwords:

CEFLS encourages and in certain instances will require that staff use password protection on their various applications and equipment. However, neither the use of passwords nor other security measures diminish CEFLS's rights to access the materials on its systems nor do they create any privacy rights for staff in the files on any system. Files may be accessed for the business purposes of CEFLS in a staff member's absence, upon authorization in writing from the Director. All passwords are the property of CEFLS, and may be changed by the network administrator or other employee designated by the Director. The following conditions govern the use of passwords:

- No employee may give any password to another employee other than the Director or the Director's designee, or to an outsider.
- No employee may use another's password.

Minors:

Internet and e-mail use and access are privileges extended to CEFLS employees. No minors under the age of 18 will be allowed to use CEFLS computers.

Breach of Policy:

The CEFLS Director and/or designated supervisory staff reserve the right, at their sole discretion, to suspend an employee's use and access upon any breach of the terms and conditions of this policy.

Filtering and Internet Safety:

In accordance with the Children's Internet Protection Act (CIPA), passed by the U.S. Legislature

in January 2001 (Public Law 106-554), CEFLS shall employ a filtering solution to block access to inappropriate content on all computers at the CEFLS office with Internet access. CEFLS certifies that a policy of Internet safety and technology protection measures shall be enforced. Users are restricted from accessing visual depictions of subject matter that is obscene, pornographic, child pornographic or harmful to minors. CEFLS shall, in furtherance of this policy of Internet safety, not allow use of the computers at CEFLS by minors.

Filtering software may be disabled for users 18 and over by a technology administrator for legitimate business and research purposes.

CEFLS cannot be held responsible for misuse of material downloaded from any online service, or for inappropriate or sexually explicit material being obtained through the network.

Confidential Information:

Information contained in CEFLS's computing and communications resources is considered confidential and proprietary to CEFLS. Employees are not authorized to disclose information or messages except in the course of discharging their duties for CEFLS. Unauthorized disclosure, use, and dissemination of personal identification information regarding any individual, including staff and patrons, and especially minors, is prohibited.

Intellectual Property:

CEFLS policy is to protect and honor the intellectual property rights of copyright holders. The potential exists for loss of control of intellectual property rights in materials that are disseminated over communication or computer systems in violation of copyright. Staff should not forward or otherwise pass along electronic materials under copyright protection without authorized permission of the copyright holder, except as permitted by law. These considerations also apply to software. CEFLS prohibits the use on any CEFLS communication or computer system of pirated or unlicensed copies of software.

CEFLS has licensed the use of certain commercial software application programs for its own business purposes. Third parties retain ownership and distribution rights to such software. No employee may create, use or distribute copies of such software, or provide passwords for non-licensed use of such software, that are not in compliance with the license agreements for the software.

Harrassment:

As with communications in all other media, no display, use or transmission of electronic communications or creation of computer files may contain sexually-oriented material, ethnic slurs, racial epithets, demeaning or obscene descriptions of individuals, or any other material that may be construed as disparagement or harassment on the basis of race, color, religion, sex, age, national origin, citizenship status, marital status, sexual orientation, disability, veteran status, or political affiliation.

Prohibited Uses:

Prohibited uses of computer and communications systems include, but are not limited to:

- using computers to perpetuate any form of fraud

- sharing confidential material, trade secrets, or proprietary information outside of CEFLS
- hacking into unauthorized websites
- sending or posting information that is defamatory to CEFLS, its services, employees and/or patrons
- introducing malicious software onto CEFLS's network and/or jeopardizing the security of CEFLS's electronic communication system
- passing off personal views as representing those of the library system
- accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a request
- making unauthorized copies of library system files or other library data system
- destroying, deleting, erasing or concealing library system files, or other library system data, or otherwise making such files or data unavailable or inaccessible to the CEFLS Director or Board of Trustees
- soliciting, advertising or proselytizing for commercial ventures, political or racial causes, outside organizations, (including philanthropic organizations but excluding CEFLS-sponsored campaigns such as for the United Way) or for other non-job related purposes

Social Media Policy:

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

The following principles apply to professional use of social media on behalf of CEFLS as well as personal use of social media when referencing CEFLS.

- Employees need to know and adhere to CEFLS policies when using social media in reference to CEFLS.
- Employees should be aware of the effect their actions may have on their images, as well as CEFLS's image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that CEFLS may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to CEFLS, its employees, or customers.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.

- Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the supervisor or Director.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized CEFLS spokespersons.
- If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with employee's responsibilities at CEFLS.
- If employees publish content after-hours that involves work or subjects associated with CEFLS, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent CEFLS's positions, strategies or opinions."
- It is highly recommended that employees keep CEFLS related social media accounts separate from personal accounts, if practical.

Staff violating provisions of this policy are subject to disciplinary action up to and including dismissal.