Buffalo & Erie County Public Library

PERSONNEL POLICIES AND PROCEDURES MANUAL

SUBJECT: Computers, Communications, & Related Technology

CHAPTER: **X**

SECTION: 1

EFFECTIVE DATE: 1/1/15

REVISION DATE: 12/20/2018

I. STATEMENT OF POLICY

The Buffalo & Erie County Public Library (B&ECPL) provides computing, networking, communication, and information resources to its staff in support of the B&ECPL's mission of connecting our diverse community with library resources that enrich, enlighten, and entertain. As a condition of providing this technology, staff members are expected to use these computing, networking, and information resources in a responsible and ethical manner. Open access to these resources is a privilege subject to acceptable use and the restrictions contained in the policies herein. These policies and procedures have been established to set forth clear expectations of acceptable use for all B&ECPL staff.

Any employee found to have violated one or more of these policies may be subject to disciplinary action, up to and including termination of employment.

II. COMPUTING, NETWORKING, & INFORMATION SYSTEMS

A. Overview

1. Internet/Intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of B&ECPL. These systems are to be used for business purposes in serving the interests of the B&ECPL and of our patrons and vendors in the course of normal operations.

2. Information is a critical asset. It must be protected from unauthorized use, modification, destruction, and disclosure. Inappropriate use of computer and information technology equipment exposes the Buffalo & Erie County Public Library to risks including virus attacks, compromise of network systems and services, compromise of bibliographic and financial information, compromise of personal information, and resultant legal issues.

3. Effective security is a team effort involving the participation and support of every B&ECPL employee and contractor who deals with information and/or information systems. It is the responsibility of every user to understand these guidelines and to conduct his or her activities accordingly.

B. Acceptable Use

1. Access to the B&ECPL's computing and network resources is provided

for use in activities relating to an employee's assigned duties, instruction, research, and public service.

2. Users must respect the rights of other users and the integrity of the systems and related physical resources. Users must also respect intellectual property, ownership of data, software licensing and contractual obligations, system security mechanisms and individuals' rights to privacy and freedom from harassment.

3. Limited personal use is permitted only during authorized break and lunch periods provided that such use does not:
    a. Interfere with B&ECPL operations;
    b. Generate incremental identifiable costs to the B&ECPL;
    c. Negatively impact the user's job performance;
    d. Involve other employment, the operation of a personal business, or other similar commercial or business activities;
    e. Violate B&ECPL policy;
    f. Violate local, state, or federal laws; or
    g. Display, print, store, or transmit electronic data that could be offensive to a reasonable person and could create a potentially hostile work environment for employees and/or visitors.

C. <u>Unacceptable Use</u>

1. Under no circumstances is an employee of the B&ECPL authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing B&ECPL resources.

2. The following are some examples of activities which are strictly prohibited (please note that this list shall not be considered exhaustive):
    a. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the B&ECPL.
    b. Copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which B&ECPL or the end user does not have an active license or express permission is strictly prohibited.
    c. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate administrator should be consulted prior to export of any material that is in question.
    d. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
    e. Making fraudulent offers of products, items, or services originating from any B&ECPL user account or computer.
    f. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing,

pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

g. Port scanning or security scanning is expressly prohibited without prior notification to and the express permission of the Information Technology Department.
h. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
i. Circumventing user authentication or security of any host, network, or account.
j. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack attempting to make the computer resources unavailable to the intended users).
k. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet.
l. Providing information about, or lists of, B&ECPL employees, cardholders, or computer users to parties outside the Library.

D. Security

1. Employees should take all necessary steps to prevent unauthorized access to information.

2. Passwords must be kept secure and accounts should not be shared unless designated as a departmental or multi-user account.

Authorized users are responsible for the security of their passwords and accounts.

3. All PCs, laptops, and workstations dedicated to a single user with personal account access should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended. Because information contained on portable computers is especially vulnerable, special care should be exercised. Laptops must be protected while traveling and should not be left unattended.

E. Monitoring and Privacy

1. Users must be aware that the data they create on the Library's systems remains the property of Buffalo & Erie County Public Library. Because of the need to protect the B&ECPL's network, the Information Technology Department cannot guarantee the confidentiality of information stored on any network device belonging to the B&ECPL.

2. For security and network maintenance purposes, authorized individuals within the B&ECPL may monitor equipment, systems, and network traffic at any time.

3. The B&ECPL reserves the right to audit networks and systems on an ongoing basis to ensure the integrity, confidentiality and availability of information and resources.

III. E-MAIL USE

A. Purpose

The purpose of the E-mail Use Policy is to insure the integrity of the public image of the Buffalo and Erie County Public Library. When e-mail is transmitted from the B&ECPL, the general public may view that message as an official policy statement from the B&ECPL.

B. Acceptable Use

B&ECPL personal or departmental e-mail accounts are established for use by authorized staff to conduct B&ECPL business or B&ECPL-related communication.

C. Unacceptable Use

1. The B&ECPL e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including, but not limited to, inappropriate comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any B&ECPL employee should report the matter to their supervisor immediately.

2. Using B&ECPL established accounts for personal e-mail is prohibited at all times.

3. Sending chain letters or joke e-mails from a Library e-mail account is prohibited.

4. Virus or other malware warnings and mass mailings from a Library e-mail account must be approved by the Information Technology Department before sending. These restrictions also apply to the forwarding of mass e-mail received by a Library employee.

5. The following additional activities are strictly prohibited:
    a. Revealing personal Buffalo & Erie County e-mail account passwords to others or allowing use of Library e-mail account by others. This includes, but is not limited to, family and other household members if a staff member has remote access.
    b. Using the Library's computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
    c. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
    d. Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.
    e. Unauthorized use or forging of e-mail header information.
    f. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
    g. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.

h. Posting non-Library-related messages to large numbers of Usenet newsgroups (newsgroup spam).

D. Monitoring and Privacy

1. Employees shall have no expectation of privacy in anything they store, send, or receive on the Library's e-mail system.

2. The B&ECPL may monitor messages without prior notice.

E. Use of Personal E-mail Accounts

1. Using the Library's resources to send/receive personal e-mail is unacceptable during work hours.

2. Personal e-mail accounts may be accessed during authorized breaks and lunch periods.

3. Employees shall not hold themselves out as representatives of the B&ECPL when engaging in non-work related communications via their personal e-mail accounts.

IV. SOCIAL MEDIA USE

The B&ECPL has adopted this Policy regarding employee use of social media in order to promote business objectives and responsible conduct.

For the purposes of this Policy, social media can be defined as a form of electronic information exchange, including a wide array of Internet resources,

websites, tools, or applications that allow collaboration, interaction, and sharing. Examples of social media include, but are not limited to the following: blogs; microblogs; wikis; photo and video sharing; podcasts; virtual worlds; social networking; social news and bookmarking; and web conferencing and webcasting.

A. Applicability

This Policy is applicable to all B&ECPL employees. Employees may not participate in social media during work time regardless of whether it is on their own personal devices, through a B&ECPL provided e-mail address or on B&ECPL equipment unless authorized to do so as part of their job. Aspects of this Policy may apply to both authorized employees participating in social media on behalf of the B&ECPL, as well as employees' personal social media activities.

B. Terms and Conditions

1. Participation in social media by authorized employees is subject to the terms and restrictions set forth in this Policy, regardless of whether the employee is accessing social media for work purposes through the B&ECPL network or B&ECPL computers or another network or computer system.

2. Social media participation by authorized employees should provide value and information that will benefit the B&ECPL, and support its policies, programs, Mission, Principles, Core Values, and Strategic Plan.

3. Employees may not engage in social media pursuant to their positions that may harm or tarnish the image, reputation, and/or goodwill of the B&ECPL and/or any of its employees, patrons, volunteers, trustees, sponsors or partner organizations.

4. The posting of anything on social media that may be construed as disparaging, defamatory or harassing of others based on their sex, sexual orientation, race, creed, color, religion, military status, gender, national origin, age, disability, arrest record, marital status, domestic violence victim status, status as an ex-offender, genetic information, or any other protected status under federal or state law, may violate the B&ECPL Equal Employment Opportunity and Anti-Harassment Policy and may be treated as a violation of same.

5. Employees may not attribute personal statements, opinions, or beliefs to the B&ECPL when participating in social media on behalf of the B&ECPL.

6. If an employee is expressing his or her beliefs and/or opinions via social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of B&ECPL.

7. Regardless of whether an employee is authorized by the B&ECPL to utilize social media, his/her personal online activities must not interfere with his/her work responsibilities and commitments or reflect negatively on the B&ECPL and/or any of its employees, patrons, volunteers, trustees, sponsors or partner organizations

8. Employees are reminded that, given current technology, lines between personal and professional use of social media sites are not always clear.

9. Employees should use good judgment and common sense at all times including when using social media, as it may reflect on the B&ECPL.

10. Employees are prohibited from revealing any B&ECPL confidential or proprietary information on social media.

11. Unless authorized, employees should not be using the B&ECPL logo or other B&ECPL intellectual property when participating in social media.

12. Employees are expected to protect the privacy of fellow employees and B&ECPL patrons. Unlawful disclosure may include, but is not limited to, the following: patron personal account information, employee personal information, and "internal only" communications.

C. Monitoring and Privacy

1. Employees participating in social media on behalf of the B&ECPL or using B&ECPL technology to participate in social media should have no expectation of privacy for such social media activities.

2. Use of social media from the B&ECPL technology systems is also subject to monitoring.

3. Employees are solely responsible for, and will be held accountable for, any and all information or materials, in any form, posted on social media. Consistent with and to the extent permitted by any applicable laws, social media sites may be monitored by the B&ECPL.

4. Employees may be subject to discipline, up to and including termination of employment, if their participation in social media (regardless of whether occurring during work time or through the B&ECPL network) violates this or any other B&ECPL policy.

V. PERSONAL SMARTPHONES, TABLETS, NOTEBOOKS AND OTHER HANDHELD DEVICES

A. Policy

Employees are not permitted to use or carry personal electronic or mobile devices including cellular phones, smartphones, tablets, notebooks, and other handheld devices, etc. during work hours, except for staff members assigned such devices for work purposes. Such devices should be kept in lockers or in secure areas, and silenced or turned off.

B. Use of Personal Devices in the Workplace

1. The Library is not liable for the loss of electronic/mobile devices brought into the workplace.

2. Staff may use these devices in break areas during breaks and lunch periods. Usage/return to lockers must not delay the return to the work area.

C. Acceptable/Unacceptable Use

The policies for acceptable and unacceptable use for computing, networking, and information systems, e-mail use, and social media use set forth herein, shall apply for use of personal smartphones, tablets, notebooks, and other handheld devices which have such capabilities.