1.0 Overview

This Acceptable Use Policy is not established to impose restrictions that are contrary to St. Charles City-County Library District (the Library)’s established culture of openness, trust and integrity. The Library is committed to protecting employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

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

Effective security is a team effort involving the participation and support of every Library staff member and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of staff computer equipment at the Library. These rules are in place to protect the employee and the Library. Inappropriate use exposes the Library to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, volunteers, interns, and other workers at the Library, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Library.

4.0 Policy

4.1 General Use and Ownership

1. While the Library’s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the Library’s systems remains the property of the Library.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. For security and network maintenance purposes, authorized individuals within the Information Technology department may monitor equipment, systems and network traffic at any time.

4. The Library reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
### 4.2 Security and Proprietary Information

1. Individual customer information may not be released per the conditions contained in Policy C280, Privacy of Library Circulation Records.

2. Keep passwords secure where applicable. Authorized users are responsible for the security of their passwords and accounts.

3. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.

4. Postings by employees from a Library email address to blogs and other online forums should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Library, unless posting is in the course of business duties.

5. All equipment used by the employee that are connected to the Library Internet/Intranet/Extranet, whether owned by the employee or the Library, shall be continually executing approved virus-scanning software with a current virus database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain various types of malware.

### 4.3 Unacceptable Use

The following activities are, in general, prohibited. Staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

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

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Installing any software or hardware on Library systems without consent of the IT Network Administrator or IT Manager.

2. Violations of the rights of any person or organization 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 Library.

3. Unauthorized 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 the Library or the end user does not have an active license is strictly prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs or malware into the network or server.

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a Library computing asset 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.

8. Making fraudulent offers of products, items, or services originating from any Library account.

9. 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. 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.

10. 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.

11. Circumventing user authentication or security of any host, network or account.

12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a staff member’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.

13. Providing information about, or lists of, Library employees to parties outside the Library.

**Email and Communications Activities (In Addition to the Library E-Mail Policies)**

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

**4.4. Social Media**

This Section is not intended to address one particular form of social media; rather social media in general, as advances in technology will occur and new tools will emerge.

**Use of Official Library Social Media Accounts**

Library employees’ use and administration of the Library’s official social media accounts as part of their regular work duties, whether using the Library’s property and systems or personal computer systems, is subject to the terms and restrictions set forth in this Policy, in addition to Policy c285.3 – Social Media Policy.

**Employees’ Personal Use of Social Media**
In accordance with applicable law, Library employees are free to express themselves as private citizens on social media sites to the degree their speech does not impair working relationships of Library employees and does not disrupt Library operations.

Library employees will not, expressly or implicitly, represent themselves as a Library employee when expressing personal beliefs or opinions on any social media forum. As public employees, Library employees are cautioned that speech conducted on or off-duty made pursuant to their official duties and responsibilities may not be protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the Library. Library employees should be aware that their social media content may reflect upon their position and the Library. Therefore, adherence to Library Policy e050 – Library Employees’ Code of Ethics, and Policy e144 – Anti-Harassment, is required in the personal use of social media.

In particular, Library employees are advised to refrain from posts containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, religion, gender, or any other legally protected class of individuals where it is likely that the public or those viewing such posts will attribute such statements or views to the Library or find that such statements or posts are likely to bring discredit to the Library or interfere with the Library's ability to perform its official functions. Library employees shall not publish information that constitutes hate speech or harassment; interferes with the work of any Library employee; creates a harassing, demeaning, or hostile working environment for any employee; or disrupts the smooth and orderly flow of work within the Library, or the delivery of services. Library employees should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Library at any time, without prior notice.

Library employees will not post, transmit, or otherwise disseminate confidential Library information to which they have access solely as a result of their employment with the Library without written permission from the Library Director. Further, Library employees shall not disclose information that is treated as a closed record under the Missouri Sunshine Law or disclose any information that is discussed during any closed session meeting under the Missouri Sunshine Law without permission from the Board of Trustees.

Notwithstanding the foregoing, this policy is not intended to restrict a Library employee’s right to discuss the operations of the Library, either specifically or generally, in accordance with Section 105.055, RSMo., and Library Policy g028.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term Definition

Malware Malware, or malicious software, is software (or script or code) designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. It is a general term used to describe any kind of software or code specifically designed to exploit a computer, or the data it contains, without consent.

Spam Unauthorized and/or unsolicited electronic mass mailings.

Effective 3.11.2020