Internet/Technology/Computer Use Policy

SCRLC has made substantial investments to make it possible for employees to electronically communicate with one another, members, and suppliers, as well as to seek information from the World Wide Web. The purpose of these investments is to help employees do their jobs in an efficient manner. To that end, this usage policy is designed to define expectations for what is acceptable and what is not when it comes to using these resources. Violation of the prohibitions contained herein may lead to disciplinary action, up to and including termination. SCRLC policies that apply to normal business behavior are applicable to use of the Internet.

Such policies include, but are not limited to, the following:

Confidentiality:

In this context "confidentiality" pertains to any type of privileged communication or information between two parties, e.g. with an attorney for a legal matter, personnel information, health-related files, or library records (note: Arts and Cultural Affairs Law. Article 45 – section §4509 provides that library records that personally identify users shall be confidential http://www.nysl.nysed.gov/libdev/excerpts/cvp4509.htm.)

Confidential Disclosure Agreement (CDA): Also known as Non-Disclosure Agreements, CDAs may be signed when two entities (e.g. a library and vendor) do business together and want to protect non-public, confidential, or proprietary information. Some employers require employees to sign a CDA that includes a clause restricting employees' use and dissemination of confidential information. SCRLC does not require a CDA to be signed though under no circumstances should an employee disseminate confidential information.

Regarding CDAs and electronic resources, the Empire State Library Network E-Resources Manifesto encourages libraries and library systems to "omit non-disclosure or confidentiality clauses from license agreements for all customers to enhance a library or consortia's ability to make informed decisions concerning pricing and content." https://www.esln.org/i2ny/e-resources/

Nonetheless, if operating under a CDA, employees should not disseminate confidential information including over the Internet to anyone not covered by it. Whenever confidential files are sent over the Internet--CDA or not--employees must exercise great care in dissemination. Due to the nature of electronic communication, it is not possible to guarantee the privacy of Internet communications. It is also easy for an email to inadvertently be sent to an incorrect address or to contain the wrong attachment files. Security and confidentiality need to be extremely high concerns for all employees.

Software Piracy

Employees are required to fulfill all license and copyright obligations of software that they download for their personal use. These software downloads become the property of SCRLC. Any employee who knowingly violates this software piracy rule is subject to termination. Prior approval for the Executive Director or a program manager is required before any software is installed on SCRLC's equipment.

Security

Employees are required to maintain all policies regarding security of SCRLC data and resources (see the section on Internet Security below).

Disclosure

Employees are expected to disclose who they are when they send email, register accounts, or conduct other Internet transactions. Attempting to subvert this disclosure policy is a serious offense.

Public Forum

Only those employees that are authorized to speak on behalf SCRLC may do so in the name of SCRLC in any news group, listserv, public forum, or chat room. An employee may mention that he/she is an employee of SCRLC in a public forum but unless authorized to speak on behalf of SCRLC should make clear that his/her comments constitute personal opinion. In all situations, an employee must refrain from making statements or rendering opinions that could affect SCRLC's reputation, confidentiality, or image.

Private Internet Use

When an employee uses the Internet on personally owned equipment and on a personal account, all confidentiality and accountability requirements of SCRLC remain in effect. An employee may mention that he/she is an employee of SCRLC, but must make clear that his/her comments constitute personal opinion. In all situations, an employee must refrain from making statements or rendering opinions that could affect SCRLC's reputation, confidentiality, or image.

Internet Access and Administration Clause

SCRLC reserves the right to limit access to the Internet for employees at any time.

Firewalls, Security Systems

SCRLC has installed a variety of systems to thwart intrusion by outside hackers. Any employee who tries to override these security measures will be subject to termination.

Unacceptable Use

Unacceptable use of the Internet may include, but is not limited to:

- Sending, receiving, or displaying text or graphics that may be construed as obscene, hateful, pornographic including child pornography, violent, unlawful or otherwise illegal material, or, with respect to the use of computers by minors, harmful to minors.
- Receiving or transmitting software, music, videos, or data in violation of copyright laws and license agreements.
- Using information obtained from the Internet in violation of copyright or without proper credit of the source (plagiarism).
- Attempting to gain unauthorized access to networks or servers.
- Disclosing someone else's password without approval.
- Using Internet communications to send or receive fraudulent, harassing, derogatory, inflammatory, intimidating, or insensitive messages, or otherwise infringe on the rights of others.
- Using SCRLC-provided Internet resources for personal gain or profit.

Compliance with the Children's Internet Protection Act:

In accordance with the Children's Internet Protection Act, the SCRLC system administrator will configure all Internet browsers to a setting that seeks to prevent users of SCRLC's computers from access to website depictions that are obscene, pornographic, (including child pornography), or, with respect to the use of computers by minors, harmful to minors. The SCRLC Executive Director will make the determination of appropriate conditions and purposes for SCRLC staff to disable this technology.

Approved by the Board of Trustees, March 21, 2014
Amended by the Board of Trustees, May 19, 2017