POLICY GOVERNING THE USE OF COMPUTER AND TELECOMMUNICATIONS SYSTEMS

This Computer and Telecommunication Usage Policy sets forth the policies of the Library with regard to its computers, telecommunications network, and data communications network (including access to and review or disclosure of electronic files and electronic mail ("email") transmitted through or stored on any part of the Library computer system), and the proper use of email and the internet.

This policy applies to all employees and any other person authorized to use the Library's computer and communications systems, whether on a permanent or temporary basis ("Authorized User"). The Library reserves the right to interpret and to modify this policy in its sole discretion at any time.

The Library provides a wide variety of computer and networking services for its employees and contractors. As an authorized user of the Library's information technology (IT) and telecommunications facilities, you are expected to use that authorization in a professional and responsible manner. It is each user's responsibility to be familiar with and abide by the provisions set forth in this policy.

The Library's computer system includes the following:

- Servers (File, Print, Email, Etc.)
- Desktop, Laptop, and Tablet Computers, and Mobile Devices
- Removable Storage Media (Flash Drives, External Hard Drives etc.)
- Printers
- Scanners
- Copiers
- Fax Machines

The Library's telecommunication system includes the following:

- Telephone System with integrated Voice Mail Facilities
- Library provided cell phones and mobile devices
- Audio & Video Conferencing Facilities
- Communication Lines (Fiber, Cable, etc.)

All hardware and software are the property of the Library. This includes any and all records, files, and electronic communications contained in these systems.

Access to System Resources

1. Hardware/Software Installation

Employees and Authorized Users are prohibited from doing the following:

- Making hardware modifications;
- Using hardware brought in from outside of the Library (including personal computers);
- Installing any software onto a Library computer; and
- Disabling the endpoint protection software.

Unauthorized equipment will be disconnected and barred from the Library's network without warning. However, if unauthorized equipment or software is required to be used for a valid business reason, the employee or Authorized User must get written approval from the Library Director or Assistant Library Director.

Endpoint protection software is installed on all Library computers. The endpoint protection software must always be running on your computer and cannot be disabled at any time. All data from external sources must be subjected to analysis of the endpoint protection software.

2. Computer Log-off

Employees and Authorized Users must abide by the following log-off procedures:

- Desktop computers: Unless otherwise designated by the Library Director or the Assistant Library Director, desktop computer musts be shut down at the end of each workday.
- Laptop or Tablet Computers: Laptop and Tablet users must shut down and power off their computers at the end of each workday. Laptop and Tablet users must place their laptop or tablet in a secure location at the end of each day.

Computer & Telecommunications Systems Usage

Use of the Library's Computer System, including but not limited to the printers, fax machines, computers, computer network and files, are to be accessed only by Employees and Authorized Users who need to use programs, files, network resources or any of the other Library equipment covered by the Library's Computer System to perform their job responsibilities in connection with their employment with the library.

The Library's computer system is to be used for job-related purposes only. Use of the Library's Computer System and equipment for personal reasons or for any non-job-related purpose is prohibited.

The Library's telecommunications system, including Library provided cellular telephones and mobile devices (if applicable), is to be used primarily for job-related purposes, although limited personal use of these systems is authorized, provided it does not interfere

with the employee's or authorized user's work or the business of the Library or cause the user to exceed the allotted minutes included in a monthly plan. If personal use causes an employee to exceed his/her allocated plan minutes, he/she will be required to reimburse the Library for the cost of the excess minutes. Minutes usage will be reviewed by the Library to ensure that the monthly plan allotment is set at a level necessary for the Employee or Authorized User to perform his/her job or work for the Library, and to ensure this level has not been inflated to cover personal minutes usage.

International calls shall not be made without the Library Director's prior written permission. Directory assistance calls made from both landline and cellular telephones should only be made when necessary for Library business.

There is no right to privacy when using the Library's computer systems or equipment or the Library's telecommunication systems. By using the Library's email, telephone, fax and/or computer systems, you waive any right to privacy in the data created, transmitted or received. The Library reserves the unlimited right to monitor, access, review, copy or delete any message, file, or document on the Library's computer and/or telecommunications system, including internet access and matter stored on any Library owned computer, laptop, table, cellular telephones, mobile devices and related media without notice and in any manner whatsoever. Employees and Authorized Users may not take any steps to prevent the Library from obtaining such access, such as changing passwords or manipulating computer programs. Routine use of "delete" or "trash" options is permitted, but employees should be aware that these options do not necessarily preclude access to the deleted material.

1. Prohibited Usage of the Library's Computer and Telecommunications Systems

The Library's computer and telecommunications systems are not to be used for economic enterprises other than the Library's, or in any way that is inconsistent with the Library's interests or the law. Use of these systems in such a way as to infringe copyrights is strictly prohibited. Employees and Authorized Users are also prohibited from sending messages (including email, text message, voice mail messages, etc.) in such a way that they appear to have originated with someone else.

The Library's computer and telecommunications systems may not be used to create, transmit, or receive any offensive or disruptive messages. Among those that are considered offensive are any messages that contain sexual implications or jokes; messages that comment offensively on a person's race, sex, age, sexual orientation, nation origin, disability, religion or any other status protected by law; messages that defame others; and messages that invade a person's privacy.

Employees should be cautious about downloading information from emails or the internet, to avoid infecting the Library's systems with computer viruses or malware. No unauthorized or unlicensed hardware or software may be used or installed on any Library computer or Telecommunications Systems (e.g., Library provided smart phones etc.).

2. Computer Network User Accounts & Passwords

Security on the Library's computer system is a top priority. Once the Library has the technical capabilities to provide each Employee with their own unique user ID, Employees must have a unique user ID and password to protect against unauthorized access to files on which they are working. (Note: that individual passwords do not prevent authorized Library representatives from accessing those files). You are responsible for any information transmitted through the Library's network under your user login. Employees should never disclose their password to any other individuals.

Users are never permitted to use another user's account without express permission of that account holder. Any attempt to log on to the network under another Employee's username and password or as a system administrator may result in cancellation of user privileges and/or discipline. Any employee or authorized user identified as a security risk may be denied access to the network.

Emails or other messages may not be sent in such a way that they appear to have originated with someone else. Log-on and other passwords may not be shared with any third party, and they may not be shared with other Library employees, except when authorized by the Library Director.

3. Confidential Information

All Library information should be treated as confidential information. Employees and Authorized Users must exercise a greater degree of caution in transmitting Library information that exists in electronic form, including patron-related information, on the computer network. Confidential information should never be transmitted or forwarded to individuals inside or outside the Library or to companies who are not authorized to receive such information. Employees are expected to use care in addressing messages (including emails, facsimiles, voice mail messages, and text messages) to make sure that such messages are not inadvertently sent to an unauthorized user or entity either inside or outside the Library. Do not forward messages containing confidential information to multiple parties unless there is a clear business need.

When transmitting confidential information to persons outside the Library, the following statement must be included: *"The information contained in this email communication contains confidential information. The information is intended for the personal and confidential use of the recipient named above. If the reader of this message is not the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone, and return the original message to us by mail at our cost. Thank you."*

Confidential information must not be displayed on a user's computer when the computer is left unattended. When computers are left unattended, they must be set to "locked" status with the password protected screen saver on, until the user returns. Flash drives or other removable media that contains confidential Library information must not be left open to access by unauthorized persons, and should be kept in locked drawers or file cabinets.

Extra precautions must be exercised when taking confidential information out of the office in a laptop computer or other portable device or smartphone. Users must never leave laptop computers, smartphones or portable devices that contain confidential information unattended when traveling.

4. Viewing and Protecting Electronic Information in Public

When viewing email or other Library content, especially on public computers, users should be aware of their surroundings so that others are not able to read messages or other information displayed on the computer screen. Users must not save passwords and must not permit the computer to automatically insert user IDs or passwords. Attachments or documents should not be saved on a public computer.

When retrieving voicemail message, whether in a Library office or in a public place, users should not use a speakerphone. Users must be aware of their surroundings so that others are not able to listen to voicemail messages.

5. Copyrighted Information

Use of the computer system to copy and/or transmit any software programs, documents, or other information protected by the copyright laws is prohibited by law and may subject you and the Library to civil and criminal penalties. Never copy software of any kind, including programs existing on the network, without prior written approval of the Library Director. Never accept copies of any software programs from other employees or persons outside of the Library, or download information from the internet without prior written approval of

the Library Director. This includes, but is not limited to, applications, games, personal Finance/Personnel software and income tax software, and any type of software used in your daily work.

6. Email and Internet Guidelines

The Library considers email to be an important means of communication, and recognizes the importance of proper email content and speedy relies in conveying a professional image and delivering good service to Library patrons.

Use of the computer network to engage in any communications that are in violation of Library policies, including, but not limited to, transmission of comments or jokes that are discriminatory, defamatory, obscene, indecent, offensive or harassing, or transmission of messages that disclose personal information about others without authorization, is strictly prohibited. Email users should use their discretion and common sense in sending emails. If you have any reservation whatsoever concerning the appropriateness of a message, you should refrain from sending it. Please note that your email messages may be read by someone other than the intended recipient(s). Some message may, at some point, require disclosure to outside parties or to a court in connection with litigation.

The following general guideline should be followed:

- All email messages should be courteous and professional.

- Email signatures must include you name, job title. Email signatures should also include your office address and telephone number. If the email discloses confidential information, the confidentiality disclaimer written above must be included below your email signature.

- Users should spell check all emails prior to transmission.

- Do not send unnecessary attachments.

- Posting an email message intended to insult and provoke, otherwise known as "flaming", is prohibited.

- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.

- Use discretion when sending personal or private information about yourself through email. Despite precautions, messages could be forwarded to unintended recipients, or viewed over an intended recipient's shoulder.

Employees should be cautious about downloading information from emails or the internet, to avoid infecting the Library's systems with computer viruses. If you have a question about whether an email can be safely opened, or whether other information can be safely downloaded, please consult with the IT Specialist, Library Director or the Assistant Director.

The Library discourages the storage of large numbers of email messages. Retention of message consumes large amounts of storage space on the Library's network and personal computers and can slow the performance of both the network and individual personal computers. In order to improve system performance and also help minimize disk storage, users should check email daily, and delete unwanted, unnecessary or outdated messages.