Liverpool Public Library Board Policy	Page 1 of 2
LPL Computers & Networks: Employee Use	Policy Adopted: 01.13.2021 Review Date: 2024

Liverpool Public Library develops and maintains staff computers, software, and networks to support its public mission. These computing resources are the property of Liverpool Public Library and are intended for library-related purposes, including direct and indirect support of the library's service mission; administrative functions; library activities; and the exchange of ideas both within the staff and the community as well as the wider local, national, and world communities. Employees have the responsibility to use these computing and network resources in a professional, ethical, and lawful manner. Employee use of computing and network resources shall be done in a manner that does not negatively affect the library's image.

Employees that have access to sensitive data resources and information are expected to protect the privacy and sensitivity of those resources and information, in accordance with the Liverpool Public Library Privacy Policy and applicable law. All data contained within Library systems is the property of the Library.

Employees are responsible for understanding security guidelines and maintaining the security of the systems and data they are using. Therefore, employees are responsible for information system activity conducted under user accounts they control.

Employees may not attempt to gain unauthorized access to computer systems within the Library. Employees may not disable or bypass security procedure. Unauthorized access or use of any Library resource may subject offenders to criminal prosecution under Federal or State law.

Security of the Library's computer systems is understood to include the control of access to information, protection of information against unauthorized access and modification, and protection of systems against the denial of service.

Software and hardware must be authorized by Computer Services. No unlicensed hardware or software may be used or installed on any library computer/system. If the employee believes certain hardware or software is necessary to perform their job duties the employee should submit a request to the Library Director.

Personal use of Library resources must be at no cost to the Library and no impact to library network operations.

Employees have no expectation of privacy when using library staff computers, software, and networks, other than that granted by applicable law or collectively negotiated agreement. Employees have no expectation of privacy of their communications, messages, and files made, transmitted, received, or stored on or through Library provided computer resources, which shall include the Library's software and networks. Even when computer resources may be password protected, there is no special confidentiality or privacy on communications, messages or files.

With no notice to employees, network administrators routinely monitor and make backup copies of certain Library computer resources, Including but not limited to the desktop, network use, communication systems, email messages, and Internet sites log, to assure the smooth functioning of the computer resources.

Network administrators have the ability to view the employee's files, messages, or other communications. With no notice to the employee, network administrators may review employee files, messages or other communications and, if misuse of the computer resources Is discovered, record or otherwise use them as a basis for disciplinary action or use them as evidence In litigation. Network administrators may also monitor employee internet activity and usage patterns to ensure that the library's computer resources are being utilized as appropriate for library purposes.

In addition to the other requirements/prohibitions set forth herein, the following list of illustrative but not exhaustive uses/conduct of Library computers, equipment and systems are prohibited:

- Making rude or hostile reference(s) regarding an individual's race, gender, age, sexual orientation, religious or political beliefs, national origin health or disability or with respect to any other class protected by applicable law;
- Any illegal activity;
- Threats or harassment;
- Slander or defamation;
- Transferring, viewing, displaying, storing, distributing, editing, archiving, or recording of any discriminatory message, image or material, or any obscene, graphic message, image or material;
- Unauthorized commercial activity;
- Accessing or attempting to access the data/files of another person unless authorized as necessary in the course of Library business;
- Using or aiding in the unauthorized use of another person's password;
- Harming or destroying date/files;
- Gambling;
- Installation of any software containing viruses or malware etc

Copyrights or licensed information shall be used only with full legal right to do so.

This Policy applies to all employee use of staff computing resources, both within the library building and from remote locations. Additional policies may govern specific computers, computer systems, or networks provided or operated by specific library departments.

The Library will review alleged violations of policy on a case-by-case basis. Anyone with information as to an alleged violation of this policy shall report said information to the Library Director, who shall investigate the matter consistent with Library policies. Violations of the policy will result in a referral for disciplinary action as appropriate. The Library may temporarily suspend, block, or restrict access to an account or workstation, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Library or other computing resources or to protect the Library from liability. The Library Director may also refer suspected violations of applicable law to appropriate law enforcement agencies.