EMPLOYEE LIBRARY COMPUTER AND E-MAIL/INTERNET POLICY

INTRODUCTION

The Jericho Public Library (the "Library") Employee Library Computer and E-Mail /Internet Policy specifies policy for the use of information resources and information technology systems. Enforcement of this Employee Library Computer and E-Mail /Internet Policy is consistent with the policies and procedures of the Library.

Being informed is a shared responsibility for all users of Library information systems. Being informed means, for example:

- Knowing these acceptable use policies and other related rules and policies;
- Knowing how to protect your data and data that you are responsible for;
- Knowing how to use shared resources without damaging them;
- Knowing how to report to technology department regarding software updates;
- Knowing how to report a virus warning, a hoax, or other suspicious activity, and
- Participating in training.

POLICY

Compliance with this policy is mandatory for all employees and contractors of the Library. This policy applies to all Library information, computer systems and data that is used for official Library business regardless of its location.

Permissions

A staff member who has a dedicated computer may be made a local administrator of such computer upon request and if a need is demonstrated. Information Technology staff may also do this at their discretion.

A staff member who has a dedicated computer will have access to a home directory and a shared network location. The shared location will be public among each department. The home directory will be private with respect to staff but accessible by the Department Head, Information Technology staff, and the Library Director.

Computers at general public service desks will automatically log into the network. These computers other than Circulation Desk computers one and two, cannot access any financial functionality or information belonging to the Library with the exception of ordering materials and services. Circulation Desk computers one and two, can collect money and run Circulation transaction reports.

Public access computers will automatically log into the network. Except for the resources necessary to manage these computers, (group policy, virus management etc.), they have no access to staff network resources.

Data Ownership and Security

Information Technology staff and the Library Director have full and unrestricted access to all information and data stored on the library network. Network access security will be place on certain folders and files in consultation with Information Technology staff, the Library Director, and the relevant Department Heads. Attempted access of unauthorized folders and files may result in disciplinary action. All files and folders stored on Library equipment are considered property of the Library.

User Accounts

New user accounts will be created using first initial and full last name as follows: First name: John, Last name: Public, username: jpublic

Resolution of a duplicate username will be resolved by adding the new user's middle initial between the first initial and last name. In the event of further conflict, a number may be placed at the end of the username.

Tampering of Records

Library staff should not tamper with any records or information that resides on any internal or external system currently in use by the Library or other staff members where permission is not granted.

Renaming User Accounts

Any staff user may request an account rename once a name change has been completed by the Library Administration Office. Such requests must be made in writing to a member of the Information Technology Department. Errors in spelling may be corrected as long as the correction matches Administration Office records – a written request must still be made to corroborate the renaming.

Retired/Terminated Employees

Once an employee is no longer a member of Library staff, the associated user account must be disabled by the end of business day of the last day of employment. The Administration Office will notify the Technical Support Department in writing of staff accounts that are to be disabled. If required, files located in the user's private directory may be assigned to a new staff member or the account may be renamed and assigned to a new user assuming similar job functions.

Library Network and Equipment

The Library reserves the right to monitor all computer equipment, traffic and actions performed in the Library network. Staff should use the network and equipment only for business purposes.

Users must:

- Protect the physical and electronic integrity of equipment, networks, software, and accounts on any equipment that is used for the Library business in any location.
- Not visit non-business related accounts.
- Not open email that seems suspicious.
- Not knowingly introducing worms or viruses or other malicious code into the system nor disable protective measures (i.e., antivirus, spyware firewalls).
- Not install unauthorized software.
- Not send restricted or confidential data over the internet or off your locally managed network unless appropriate encrypted.
- Not connect unauthorized equipment or media, which includes but not is limited to: laptops, thumb drives, removable drives, wireless access points, PDAs, and MP3 players.
- Not harass other users using computer resources, or make repeated unwelcome contacts with other users.
- Not display material that is inappropriate in an office environment consistent with the Library policies.
- Not use unauthorized streaming of audio, video, or real time applications such as: stock ticker, weather monitoring or internet radio.

Technology Department must allow established procedures for protecting files, including managing passwords, using encryption technology, and storing back-up copies of files.

Email

All email accounts given to the employees are the property of the Library. As such the Library reserves the right to actively monitor, view and share both incoming and outgoing correspondence sent from staff email accounts. Library staff members should not use Library email addresses for any personal or non-Library related purposes. All email should be composed according with our behavior policy.

Social Media Accounts

Social media accounts belonging to and representing the Library are restricted to business use only. Personal opinions or controversial statements should not be put on Library social media accounts without expressed written permission from the Library Director.

Password Policy

All staff user accounts are to be subject to the password policy stipulated below:
Number of day(s) before a password may be changed: 1
Minimum number of characters in a password: 6

Complexity Requirements:
Passwords must not contain any part of the staff member's name and/or username.
Passwords must contain characters from three of the following four categories:
Uppercase (A through Z)
Lowercase (a through z)
Digits (0 through 9)
Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

Lost/Forgotten Passwords:
If a user loses or forgets their password, they must notify the Technology Department to reset that password. The Tech Support Department will reset the password, and require that the user change the password after logging in, using the aforementioned complexity requirements. At their discretion, the Tech Support Department may require a written request for this change

______________________________ Date ______________________
Signature

Adopted by the Board of Trustees of the

Jericho Public Library	March 13, 2000
Revised	July 11, 2016
Revised	September 8, 2020