Woodstock Public Library Policy

Policy Name: **Computer and Technology Acceptable Use Policy**

Category: **Personnel**

Version: **11 April 2023**

POLICY STATEMENT AND RATIONALE

The purpose of this policy is to outline the Board's expectations regarding the use of the Library's information technology resources for staff and volunteers, ensure the integrity of the Library's computer infrastructure and data, and identify the purposes, methods and circumstances under which the Library may electronically monitor its employees.

This policy does not cover the use of the Library's video surveillance system, which is a separate policy.

SCOPE

This policy applies to all staff and volunteers of the Woodstock Public Library and external organizations that may directly or indirectly require access to Library computer IT resources.

DEFINITIONS

Board means the Woodstock Public Library Board.

CEO means the Chief Executive Officer of the Woodstock Public Library.

City means the City of Woodstock.

City IT means the Information Technology department of the City of Woodstock.

Computer IT Resources means all Library information technology systems, or applications that store, process, or transmit information; all network infrastructure and computer hardware, storage, software and applications, mobile devices, and telecommunications systems.

Data means all information residing on Library networks, external storage, and devices that include but are not limited to files, voicemail, databases, transactional streams, and logfiles.

Electronic Monitoring means all forms of employee and assignment employee monitoring that is done electronically.

Library means the Woodstock Public Library.

Staff means an employee of the City of Woodstock Public Library.

POLICY, PROCEDURE, AND IMPLEMENTATION

1.0 Statement of Authority

1.1 This policy is in accordance with the *Public Libraries Act, 1990*, and the *Employment Standards Act, 2000*.

2.0 Responsibility

2.1 The Library CEO is responsible for implementing the appropriate procedures in accordance with this policy.

2.2 Under the authority of the CEO, responsibility for the administration, monitoring and security of the Library's computer resources and data rests with the Manager of Operations.

3.0 Guiding Principles

3.1 Use of the Library's computer IT resources and Internet access are provided to staff as business tools to assist them in performing their work-related duties.

3.2 While carrying out library business, staff and volunteers are provided access to the Library's computer network and data based on the following principles:

Need to Know: Staff and volunteers will be granted access to systems and data that are necessary to fulfil their roles and responsibilities.

Least Privilege: Staff and volunteers will be provided the minimum privileges necessary to fulfill their roles and responsibilities.

3.3 Computer equipment, devices and electronic records are the property of the Board. The Board has the right to access and monitor all equipment, devices and electronic records.

3.4 The use of the Internet and email systems shall comply with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*, the *Public Libraries Act* and other applicable laws.

4.0 Staff Responsibilities

4.1 Staff are expected to use their best judgement and demonstrate a sense of responsibility when using Library computer IT resources.

4.2 All work undertaken shall be performed in an ethical and lawful manner, demonstrating integrity and professionalism.

4.3 Staff will abide by the limits set out in the "Unacceptable Computer Resources Use" section of this policy.

4.4 Staff are responsible for safeguarding their passwords and for all transactions made using their passwords. Individual passwords, logon ID, internal network configurations, addresses, and system names must not be transmitted in email messages, printed, stored online, or shared with others. Staff suspecting that their access passwords have been compromised should take steps immediately to change their password and notify the Manager of Operations.

4.5 Abuse of this policy is subject to appropriate discipline, which may include dismissal of an employee or termination of a contractor's contract.

5.0 Cyber Training

5.1 All staff are required to take mandatory cyber security training on the use of library systems during their orientation period.

6.0 Authorized Licenced Software

6.1 Only licenced software and registered shareware acquired by, and paid for by the Library, is to be operated on the Library's computer network. In order to protect the integrity of licences and network security, staff are expected to adhere to the following guidelines:

a) Only licenced software authorized by the Manager of Operations is to be installed on Library computers.

b) Board licenced software is not to be copied or transferred to home computers without the consent of the Manager of Operations.

c) No software of a personal nature is to be maintained on the Board's computer network.

7.0 Personal Use of Computer IT Resources by Staff

7.1 Limited and occasional personal use of the Library's computer IT resources are permitted within these general guidelines:

a) Personal use will be on an employee's own time.

b) Staff will not use Library IT computer resources for private business purposes.

c) Personal use will not interfere with any work-related activity or impact network operations.

d) Employees will supply their own expendable materials.

e) Staff acknowledge that the Board retains the right to access and monitor their activities as deemed necessary by the Board.

8.0 Unacceptable Computer Resources Use

8.1 These restrictions apply to all internal and external use of all computer resources and data by all users, regardless of geographical location. The following practices are improper and unacceptable:

a) Transmitting or releasing sensitive, confidential, proprietary, or privileged information to anyone not authorized by the CEO or their delegate to receive it.

b) Sending, storing, or soliciting communications containing material that is fraudulent, harassing, pornographic, profane, obscene, vulgar, intimidating or unlawful.

c) Participating in controversial or inappropriate internet discussion groups such as pornographic, hate-based, or terrorist discussion groups.

d) Downloading copyrighted content from the internet, except for research purposes or non-commercial use.

e) Interfering with, removing, or bypassing any security features or devices designed to protect data, whether Library data or not, from viruses, unauthorized external access, or other security risks.

f) Intentionally broadcasting messages or participating by propagating non-business documents/messages such as chain letters or knowingly transmitting destructive programs (viruses and/or self-replicating code).

g) Sending mass mailings that have not been authorized by an appropriate Library manager.

h) Disrupting the Library's ability to perform its mission.

i) Engaging in any activity intended to cause congestion or disruption of networks and systems.

j) Attempting to send anonymous transmissions or to falsify information regarding the originator by any means including use of another user's identification or login ID.

k) Downloading and installing software from the internet, CD-ROMs, thumb drives or elsewhere onto computer resources without the Manager of Operations' written permission to do so.

l) Using any software without a valid licence.

m) Distributing or copying software without prior written permission from the Manager of Operations.

n) Sending or soliciting transmissions of commercial or personal advertisements, solicitations, promotions, political material, or other material for unauthorized or personal use.

o) Storing personal data.

p) Conducting any personal business venture or money-making activity.

q) Connecting unauthorized devices to the Library's network without obtaining prior approval from the Manager of Operations.

9.0 Electronic Monitoring of Employees

9.1 The Library has the capability to monitor Library staff, but will only access data in the following cases:

a) Staff Safety: Staff who work alone at night in the building are monitored to ensure their safety. Staff are monitored for sudden falls or periods of lengthy inactivity that might be an indication of a medical emergency.

b) Systems Performance and Statistics Collection: Staff activity may be monitored to compile metrics in order to analyze and improve library operations and workflow, or to report statistics to the Board and Ministry.

c) Investigations: The Library may access and monitor system data in order to investigate patron misbehavior and staff performance.

d) Building Security: The Library may access and monitor data concerning access to the building to ensure the security of the library building.

e) Asset Management: The Library, in consultation with and assistance from City IT, may access and monitor location tracking software on City or Library owned technology, such as cellular devices and hotspots.

10.0 Disclaimer

10.1 This policy may be amended or revised at any time by the Board.

10.2 This policy supersedes all other Board policies with regard to the use of the Library's computer IT resources and data by staff and volunteers.

10.3 This policy is not meant to be exhaustive; additional rules, procedures and guidelines regarding the use of the Library's computer IT resources and data, may be introduced at any time, as deemed necessary by the CEO.

10.4 The Manager of Operations may change, bypass, or disable an employee's password or other security mechanisms at any time without permission or advance notice to the employee.

RELATED DOCUMENTS AND POLICIES

Woodstock Public Library – Video Surveillance Policy
Woodstock Public Library – Access to Information and Protection of Privacy Policy
Woodstock Public Library – Disconnect from Work Policy
Employment Standards Act, 2000, S.O. 2000, c.41
Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56

DOCUMENT REVISION RECORD

Adoption Date: 13 September 2022
Review Cycle: Once per Term
Last Reviewed: 11 April 2023
Resolution No.: 23-28