BRACEBRIDGE LIBRARY POLICIES

Policy Number: OP-44 Title: Staff Use of Technology Board Approval Date: January 2022	Category: Operational Policy Replacing: N/A Year of next review: 2026

PURPOSE:

The Bracebridge Library recognizes the importance of computers, devices and the Internet as work tools and sources of information. The Library supports the use of computers, devices, the Internet and email by staff in their work while recognizing the need to protect its network, systems and resources.

The purpose of this policy is:

- To ensure use of technology resources is consistent with the Library's values and operations.
- To instruct staff in the efficient, effective and secure use of the technologies and offer guidelines on acceptable use.
- To ensure staff understand inappropriate uses that are not acceptable may result in loss of privileges, and/or disciplinary action up to and including dismissal, depending on the severity of the infraction.
- To protect the Library and its information technology infrastructure against hazards such as unauthorized access, malicious manipulation and/or destruction of information/data, virus invasion, inappropriate use, litigation due to misappropriation of software and/or data, and/or inappropriate disclosure of personal information.

DEFINITIONS:

Computer Resources: Includes, but is not limited to the Internet, software, printers, computer equipment, devices, and Internet Service Providers (ISPs) including cloud based-resources, etc.

Designated Communicator: A Bracebridge Library employee who is authorized by the CEO, or their designate, to participate in social media for approved business purposes.

Devices: Examples include, but are not limited to computers, touch screen tablets, phones running on all platforms.

Social Media: A term that refers to third-party internet based applications, websites and databases that enable collaboration and sharing of opinions, images, information, experiences and conversations among staff. Social media channels include, but are not limited to Blogs, Forums, Facebook, Twitter, Instagram, Tik Tok, YouTube, Pinterest, Vimeo, Flickr, LinkedIn, Hoot Suite, etc.

Staff: This includes full-time, part-time and casual staff, as well as volunteers and any contractors and consultants including their affiliated third parties who may have access to library systems or networks.

POLICY STATEMENT

SCOPE:

This policy addresses use of Library housed or issued computer equipment, devices, software, operating systems, applications, use of the Internet, email, and use of the Library's network, etc.

GUIDELINES:

Acceptable Use of Technology and Employee Accountability

The Library provides staff with technology resources to support their work and learning on behalf of the Library. Acceptable use of technology resources includes the following:

Primarily for Work and Learning

The technology resources provided by the Library are intended primarily to support Library operations, work and ongoing professional development.

Personal Responsibilities

By using the Library provided technology resources, staff assume personal responsibility for appropriate use and agree to comply with this policy, and other applicable policies, licenses, acceptable use terms, contracts and agreements as well as provincial and federal laws and regulations.

It is the responsibility of all staff to read and understand the applicable terms of use of the systems they use. All staff are required to acknowledge that they have read and will act in accordance with the Policy and Guidelines.

All staff have an obligation to protect passwords and access codes and must not disclose to unauthorized individuals or the public.

All employees are responsible for reporting inappropriate use, behavior or communications to the CEO, or their designate.

Limited Personal Use

Occasional and incidental personal use of Library technology resources is permitted during breaks provided that such use does not adversely affect the daily work of the Library. Prolonged use of technology for personal use is not permitted. Business use or use for profit not related to Library work is not permitted. Staff are responsible for exercising good judgment regarding reasonableness of personal use. If there is any uncertainty, staff should consult the CEO, or their designate.

Ownership

All computer equipment, devices, licensed versions of software programs and electronically created files and emails are considered the property of the Library, until such time that they are removed from the Library's inventory. Content and work done on the Library's systems and technology resources is owned by the Library. Making copies of software that is under the Library's license is prohibited.

Inappropriate Use and Inappropriate Material

Inappropriate use includes, but is not limited to, using the Library technology resources for:

- Creating, accessing, sending, uploading, downloading, posting, loading or saving inappropriate material;
- Creating, sending, uploading, posting or loading information that constitutes threats, harassment, libel, slander, defamation or other similar acts;
- Creating, sending, uploading, posting or loading information that constitutes a nuisance, including spamming and virus distribution;
- Downloading software that has not been approved by the CEO, or their designate; and
- Using the Library's facilities without proper authorization

Inappropriate material may include, but is not limited to:

- Any pornographic or violent material including text and pictures;
- Hate propaganda as defined by the Canadian Charter of Rights; and
- Other material prohibited under legislation and Library policies.

Personal Hardware and Software Installation

Staff owned hardware and software is not to be installed on the Library's computer equipment.

Passwords & Terminal Protection

Passwords are an important aspect of computer security. They are an integral part of the front line of protection for staff accounts and network security. All staff with access to computer terminals are required to safeguard passwords to staff terminals, network connections, email accounts, etc.

Passwords may not:

- be revealed over the phone to anyone;
- be shared in an mail message;
- be shared with fellow employees or volunteers;
- stored in the "Remember Password" feature of applications;
- written down and stored in the office; or
- be stored in a file on ANY computer system unencrypted.

If an account or password is suspected to have been compromised, it must be changed immediately and reported to the CEO, or their designate.

Privacy and Confidentiality

The Library may access and use all information and data stored on and communicated through its technology resources for legitimate purposes including:

- to facilitate work in a staff absence;
- to conduct routine technical administration;
- to investigate suspicions of improper system use; and
- to comply with legal obligations.

Staff who engage in personal use of the Library's technology resources are deemed to accept that the Library has this right of access and may raise no expectation of privacy that prevents the Library from accessing and using information and data for its legitimate purposes.

Upon commencement of work, all staff must complete an acknowledgement of having read, understood and agreeing to the terms of this policy.

Monitoring

As a means of protecting the security of the Library computing environment and facilitating systems management, the Library may monitor staff computer use/equipment and data stored or communicated through technology resources to ensure appropriate use. Any such monitoring requiring access to staff documents, browsing history or email accounts, will only be undertaken with the authorization of the CEO, or their designate.

Bracebridge Library Email Accounts

Appropriate Use of Email

The Library's email system is for Library business communication. The following are examples of authorized uses of email: Communication with staff, other official bodies and vendors as required by the position:

- Responding to enquiries;
- Participating in professional, job related research ;
- Distributing work related correspondence ;
- Accessing approved job related distance learning opportunities; and
- Participating in job related listservs, mailing lists, blogs, etc.

Message Standards

All correspondence sent from the Library should be treated as a professional document. As such, all messages directed to recipients outside of the Library should include a signature line containing the following elements and reflecting the Library's logo:

- Name;
- Position;
- Department;
- Email address;
- Name of library; and
- Phone number

Viruses, spyware, malware, ransomware and Email

Emails from known and unknown sources may contain viruses that can affect the Library's network. It is the responsibility of staff to exercise caution when receiving any email attachments.

Internet Use

Appropriate Use of the Internet

The following activities are examples of appropriate use of the Internet by all staff:

- Research related to customer information enquiries;
- Research related to developing resources for the Library's publications, website; and

- Other sites accessed as required to perform job duties

Unfamiliar Media

Computer viruses may be spread unintentionally through the use of unfamiliar media such as flash drives, external hard drives, memory cards, etc. Such incidents may also occur through opening an attachment from an unfamiliar address. Such actions may inadvertently jeopardize the network and computer systems throughout the library. As such, staff must:

- Not insert any form of unknown media into a networked or staff computer;
- Analyze all unknown forms of media on a separate laptop, available from the CEO, or their designate, which has no connection to the Library network;
- Not open any attachments contained in an email from an unknown source; and
- Not remove any filters or firewalls set in place on the library network by the Library IT staff or IT contractors.

Should any staff need support in analyzing an unfamiliar form of media or email from an unknown source, they are to immediately contact their direct supervisor or the CEO, or their designate, for advice on how to proceed safely.

Contravention of Policy

If the Library suspects a policy violation, the Library may restrict access to technology resources pending the completion of an investigation. If the Library finds a policy violation, the Library will exercise its rights to take appropriate disciplinary action depending on the severity of the infraction including, but not limited to:

- Verbal or written warning;
- Rescinding of email or Internet accounts;
- Restricted access to technology resources; and
- Disciplinary action up to and including dismissal

Authorization must be obtained from the CEO, or their designate, prior to commencing an investigation into inappropriate use of technology resources.

PREVIOUS REVISIONS: None

RELATED DOCUMENTS: Canadian Charter of Rights and Freedom