



Section of Policy Manual: Personnel	Policy No. : PER-02
Subject: Staff Use of Technology	Policy Approval Date: April 11, 2024 Date First Approved: November 9, 2017
Year of next review: April 2028	Last Review/Revision Date: March 2024

The Gravenhurst Public Library Board recognizes the importance of computers, the internet and social media as work tools and sources of information. The Library provides computers, devices and access to the internet needed by employees to work while recognizing the need to protect its network, systems, resources and the Library’s profile in the community.

This policy covers employee use of library computers, devices, e-mail system and networks. Employee use of social media is addressed in policy **PER-03**.

Section 1: Personal Use

1. While working in the Gravenhurst Public Library, employees must refrain from online activities that don’t bring value to the Library. Employees may make reasonable personal use of the Library’s computer equipment, access to the internet and e-mail on their own time, provided it does not adversely affect their work or the work of others and has minimal effect on the library’s resources.
2. Computer resources cannot be used for private financial gain or commercial purposes.
3. Making copies of software is prohibited.
4. Downloading software or attachments onto a work computer increases the risk of compromising the network. Employees should use caution when downloading files or software.

Section 2: Business Use

1. Employees are encouraged to avail themselves of the internet including using social media for the benefit of the Library. This may include general research



on work related issues, following social media as part of ongoing professional development, employee or user training, and participating in online forums.

2. Any correspondence sent from the Library's email address, or when an employee is identified as a member of the staff of the Library, should be treated as a professional document.
3. Employees must observe the Library's standard of confidentiality (e.g. privacy legislation) when communicating electronically.
4. Downloading software or attachments onto a work computer increases the risk of compromising the network. Employees should use caution when downloading files or software.
5. Employees have an obligation to protect systems and data. Passwords and access codes must not be disclosed to unauthorized employees or the public.
6. Employees must complete all required ITS Security Awareness Training by the assigned deadlines.

Section 3: Prohibited Use

1. The Library's computers, network and access to the internet are not to be used to:
 - a) undertake deliberate activities that waste employee time or networked resources
 - b) introduce any form of malicious software into the network
 - c) visit internet sites that contain obscene, hateful, pornographic or illegal material
 - d) perpetrate any form of fraud i.e. software, film or music piracy
 - e) access unauthorized areas
 - f) send offensive or harassing material

Section 4: Misuse

1. Employees are accountable to the CEO/Chief Librarian for use of the library's computer network and internet access.



2. The CEO/Chief Librarian, or their designate, will investigate any suspected misuse of resources.
3. If there is a need to monitor or access non-work related files, an employee will normally be asked for their consent. There may be exceptions such as when there is reason to believe the law has been broken.
4. The CEO/Chief Librarian will decide, in light of the outcome of an investigation of possible misuse of technology resources, if disciplinary action is appropriate and act in accordance with established disciplinary procedures.

Related Documents:

GPL Policy ***PER-03 Staff use of Social Media***

GPL Policy ***PER-12 Employee Code of Conduct***

GPL Policy ***PER-10 Professional Development Performance Evaluation***

GPL Policy ***PAT-01 Privacy, Access to Information, and Electronic Messages Under CASL***

Municipal Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. M56

Municipal Freedom of Information and Protection of Privacy Act R.R.O., 1990, Regulation 823