## 6.5 Internet Acceptable Use Policy

### Intent

The purpose of this policy is to outline and ensure that internet resources are used appropriately when conducting business on behalf of the employer. Within this policy, "internet resources" include, but are not limited to: Web access, FTP (file transfer protocol) servers, the intranet, and the employer domain names and IP addresses.

### Scope

This policy applies to all employees always and without exception.

Unionized employees are requested to refer to their current Collective Agreement for specific information pertaining to this Internet Acceptable Use Policy. Where a Collective Agreement is silent on the issue, this policy shall dictate the requirements for unionized employees. In situations where the directions of this policy cover issues also in the Collective Agreement, the Collective Agreement will be the final authority.

### Guidelines

Computer equipment and internet access is the property of the employer and must be used in accordance with company policies. Gaming, Facebook, dating sites such as Plenty of Fish, pornographic or defamatory sites and file sharing of any kind are strictly forbidden. Usage must relate to the employee's function within the company. Misuse of the internet will result in disciplinary actions up to and including immediate dismissal.

- Internet access is managed via individual user accounts and confidential passwords. With respect to account setup and network administration, department managers are responsible for identifying and recommending network access levels for staff members in their department.
- All user names and passwords for must be supplied to management.
- If an employee forgets, or believes that their password has become compromised, the employee must inform management immediately. Management shall confirm the user name, reset the password, and inform the employee of changes made, and the procedures for changing their password.
- When employment is terminated, management will notify the department or employee in charge of that location's information technology to ensure the removal of the former employee's access to email and internet resources. This is an important measure in protecting the safety and integrity of the employer's resources.

Employees may use the internet only to complete their job duties, under the purview of their business objectives. Permissible, acceptable, and appropriate internet-related work activities include:

1. Researching, accumulating, and disseminating any information related to the accomplishment of the user's assigned responsibilities.
2. Conducting professional development activities (e.g. news groups, chat sessions, discussion groups, posting to bulletin boards, webinars, etc.) as they relate to meeting the user's job requirements. In instances where the personal opinions of the user are expressed, a disclaimer must be included asserting that such opinions are not necessarily those of the employer.

Internet use shall comply with all federal and provincial laws, and will not violate other policies. Inappropriate and unacceptable Internet use includes, but is not limited to:

1. Usage for illegal purposes, such as theft, fraud, slander, libel, defamation of character, harassment (sexual and non-sexual), stalking, identity theft, online gambling, spreading viruses, spamming, impersonation, intimidation, and plagiarism/copyright infringement.
2. Any usage that conflicts with existing policies and/or any usage that conflicts with the employer's mission, goals, and reputation.
3. Downloading unreasonably large files or streaming videos that may hinder network performance.
4. Accessing, downloading, or printing any content that exceeds the bounds of good taste and moral values (i.e. pornography).
5. Engaging in any other activity which would in any way bring discredit, disrepute, or litigation upon the employer.
6. Engaging in personal online commercial activities, including offering services or products for sale or soliciting services or products from online providers.
7. Engaging in any activity that could compromise the security of host servers or computers. All passwords shall not be disclosed to, or shared with, other users.
8. Engaging in any fundraising activity, endorsing any products or services, or participating in any political activity, unless authorized to do so as part of completing one's assigned job duties and responsibilities.
9. Allowing unauthorized or third parties to access the employer's network and resources.

This policy allows room for limited and reasonable personal use of the internet. This privilege may be revoked at any time where it has been identified that this benefit has been abused.

Personal use shall not:

1. Have a negative impact on user productivity or efficiency.
2. Interfere with normal business operations.
3. Exceed reasonable time limits, and will be limited to the employee's break and lunch times.
4. Cause expense or network slow downs.
5. Compromise the integrity and security of the employer's resources or assets.
6. Conflict with any existing policies.

Employees must comply with the following security guidelines, rules, and regulations:

1. Personal files or data downloaded from the internet may not be stored on hard drives or network file servers.
2. Video and sound files must not be downloaded from the internet unless their use has been authorized for the purposes of conducting the employer's business.
3. Users must refrain from any online practices or procedures that would expose the network or resources to virus attacks, spyware, adware, malware, or hackers.

Violations of this Internet Acceptable Use Policy may result in one or more of the following:

1. Temporary or permanent revoking of access to internet resources and/or other IT resources.
2. Disciplinary action up to and including suspension or termination of employment.
3. Legal action per federal or provincial laws.