Section 6 - Technology

6.1 Communications Policy

Intent

This policy is intended to cover office telephones, cellular telephones, PDAs, Blackberries, two-way radios, and all other forms of portable communication devices. This policy shall also outline standards, guidelines and procedures for appropriate use related to such devices.

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 Communication 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

The employer provides office phones, computers and cell phones to eligible employees in order that business operations may be conducted smoothly and efficiently. Whether utilizing an office landline or company-provided cell phone, employees are expected to use such devices for the purpose they have been provided for.

Communication devices and service packages used to conduct business must be used responsibly, ethically, and cost-effectively always, therefore, the following policy statements must be adhered to always:

1. Employees are directed to utilize office telephones, their personal or company-supplied cellular phones for business purposes only during regular business hours.
2. Employees are asked to use the same discretion in using personal cell phones as they use with company phones. Excessive personal calls during the workday, regardless of the phone used, can interfere with employee productivity and be distracting to others.
3. Employees are requested to inform their friends and family of the company's Communication Policy to avoid unnecessary incoming landline or cell phone calls during the work day.
4. The employer shall not be liable for the damage or loss of personal cellular phones brought into the workplace.
5. Employees are strictly prohibited from using cellular phones for any other available purpose (e.g. internet access, gaming, music) during business hours. These functions may be used during scheduled breaks or lunch periods in non-working areas.

RELEVANT DOCUMENTS

Personal Mobile Device Policy

Management Mobile Device Policy

6.2 Management iPhone Policy

Intent

The employer will, at its discretion and in accordance with this policy, provide management employees with mobile devices and telecom carrier services, at the employer's expense, for the primary purpose of conducting company business. All mobile devices that are paid for in full or in part by the employer are the property of the employer and the employee is responsible for ensuring the appropriate use of the mobile device, as well as the security and safe keeping of the mobile device as outlined in this policy.

Scope

This policy applies to management employees who have been provided with a mobile device at the expense of the company and includes any form of wireless communication device provided to the employer to the employee that is capable of transmitting packet data. The employer may at its discretion, choose not to provide a mobile device to a management employee, even though the employee may be eligible.

Unionized employees shall adhere to their current Collective Agreement for policies governing mobile device use. Where the Collective Agreement is silent, bargaining members shall refer to the contents of this policy. In situations where the directions of this policy cover issues also in the Collective Agreement, the Collective Agreement will be the final authority.

Guidelines

The employer agrees to provide its management employees with a mobile device provided through a national carrier. The monthly usage costs for the mobile device will be paid by the company. The employer reserves the right to deduct from the employee's pay any monthly charges that are more than monthly usage/consumption targets, if such monthly charges are proven to be non-business related.

Employees are responsible for staying within their allotted mobile allowance. Charges associated with using a company provided mobile device for personal communications including text messages, email and voice calling will count towards the monthly consumption limit. Therefore, personal use of a company provided mobile device should be minimized. Mobile device usage reports will be communicated to the individual employee anytime there is an overage in the established and agreed upon allowable charges.

Company provided mobile devices remain the property of the employer and are therefore revocable at any time. Company provided mobile devices and all packaged accessories must be returned to the employer upon resignation or termination of employment and must be in proper working order and like new condition. Any cost to repair or replace a company provided mobile device will be covered by the employee unless there is deemed to be a manufacturing defect.

The employer expects its employees to use their mobile devices prudently during working hours. Excessive use of mobile devices for non-business purposes can mean a decline in efficiency; it is to the benefit of all to consciously restrict personal use of mobile devices during working hours.

Management mobile device spend will be monitored monthly. Access to the telephone numbers which have been dialed by the employee will only be requested when non-compliant activity has been detected in compliance with corporate usage and privacy laws.

The safety of employees is critical to our ongoing success. Therefore, the employer requires all employees with a company issued mobile device to utilize hands-free equipment when using the mobile device while operating a vehicle. Employees should also use voice activated calling or pre-programmed numbers to prevent distraction from safe driving. Any other mobile device enabled activity that prevents an employee from focusing on driving such as surfing the internet, text messaging, checking email, use of applications, or other activities, is prohibited.

No employee is to use company-owned mobile devices for illegal transactions, harassment, or obscene behavior, in accordance with other existing employee policies.

The following rules always apply for company-issued phones and other mobile devices:

- Company-issued phones are to be used for business purposes only and be preserved in as close to perfect condition as possible
- The download or upload of inappropriate, illegal or obscene material through a corporate internet connection is prohibited
- The use of a cell phone's camera or microphone to record confidential information is strictly prohibited
- It is recommended that employees turn off their phones/devices or keep them on vibrate to minimize disruption in the office

The company retains the right to monitor employees for excessive or inappropriate use of their company provided mobile devices.

For an action that constitutes a breach of security, violation of the confidentiality policy or cause of an accident the employee may face severe disciplinary repercussions up to and including termination. Failure to comply with this policy will result in appropriate remedial action, which may include but is not limited to revocation of privileges or disciplinary action, including suspension or termination of employment.

RELEVANT DOCUMENTS

Communications Policy

Personal Mobile Device Policy

6.3 Personal Mobile Device Policy

Intent

This cell phone policy is designed to detail the company's attitude towards the use of personal mobile devices in the workplace. We recognize that mobile devices and smartphones have become an integral part of everybody's life and believe they may be a great asset in the workplace if used correctly (for productivity apps, calendars, business calls etc.).This policy clarifies the allowances and restrictions of personal mobile device use.

Scope

This policy applies to all employees always and without exception.

Unionized employees shall adhere to their current Collective Agreement for policies governing personal mobile device use. Where the Collective Agreement is silent, bargaining members shall refer to the contents of this policy. In situations where the directions of this policy cover issues also in the Collective Agreement, the Collective Agreement will be the final authority.

Guidelines

Despite their benefits, mobile devices may cause significant problems in the workplace. The reasons for this include:

- The distraction of employees by regularly checking their phones
- The time subtracted from actual working hours by the mundane use of mobile devices
- The interference on colleagues' jobs by speaking on the phone
- Misuse of the company's internet connection

The employer expects its employees to use their mobile devices prudently while working. Excessive use of cell phones for non-business purposes results in a decline in the employee's efficiency which will show up in their performance reviews. It is therefore to the benefit of all to consciously restrict personal use of mobile devices.

- The following rules always apply for personal phones and other mobile devices:
- The use of a phone for any reason while driving a vehicle is prohibited.
- The use of mobile devices within earshot of someone else's work space during work hours is not allowed.
- The download or upload of inappropriate, illegal or obscene material through a corporate internet connection is prohibited.
- The use of a cell phone's camera or microphone to record confidential information is strictly prohibited.
- Employees are prohibited use of their phones within the view or ear shot of any guests/customers.
- It is recommended that employees turn off their phones/devices or keep them on vibrate to minimize disruption in the office.

The use of phones and other mobile devices should be reserved to:

- Breaks or lunch hour
- While in a parked company vehicle
- To briefly check important messages

- In an emergency, to make brief personal calls away from the working space of colleagues/guests/customers
- To make business calls
- To use productivity apps or other useful job tools

The company retains the right to monitor employees for excessive or inappropriate use of their mobile devices. If it is discovered that an employee's mobile device usage causes a decline in productivity or interferes with work, the company will further restrict that employee from using their mobile device(s) while onsite and during their work hours.

For an action that constitutes a breach of security, violation of the confidentiality policy or cause of an accident, the employee may face severe disciplinary repercussions up to and including termination. The employer is not responsible for the loss, theft or damage to a personal device of any employee.

RELEVANT DOCUMENTS

Management Mobile Device Policy

Personal Mobile Device Policy

6.4 Corporate Software Policy

Intent

The employer regularly requires the use of various software packages to conduct business effectively. As such, when licensing third party software, the employer will respect all copyright protection legislation.

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 software 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

The employer will adhere to all applicable legislation and regulations in the performance of our corporate activities, including copyright legislation and software license agreements.

The employer strictly prohibits the creation and/or use of pirated software, illegal file sharing, downloads and/or uploads of copyright materials and will apply appropriate disciplinary actions in the event of any breach of this policy. Unauthorized duplication of software can create unnecessary legal liability for both the company and the employee in terms of both civil and criminal penalties under Canada's Copyright Act.

All purchased software must be registered to the employer and the department that will utilize it. To avoid issues involving staff turnover, the employer will not register software in the name of the individual user.

The employer shall retain the original copy of the purchased software, as well as all applicable warranty information, user manuals, license agreements, and receipts in an appropriate location for storage. The employer shall create and maintain a backup copy for use in an emergency.

Any materials downloaded must be scanned using anti-virus software prior to installation.

If an employee requires the use of software for working from home, they must contact management to determine if the license agreement will allow for this.

Employees are prohibited from installing or otherwise using software or other copyrighted material that has not been authorized by the company. As such, any software brought from home cannot be used in the employer computers.

The employer may perform a software audit on any company owned computer, at any time, to ensure compliance with the Corporate Software Policy.

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.

6.6 Email Best Practices Policy

Intent

The employer has adopted this policy to ensure that employees are provided with guidelines for the appropriate use of email communications.

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 email best practices. 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

The employer strives to convey a professional image always, and will work to ensure that all forms of communication meet specific standards of professionalism, and are created using best practices. Employees are required to adhere to the following standards pertaining to email communication on behalf of the company:

1. Employees are expected to ensure that all communications will be created using a consistently high level of professionalism.
2. Email communications must be polite, and begin with an appropriate greeting (e.g. Hello, Dear, or Good Morning, etc.).
3. Ensure that all messages use appropriate language. Inappropriate language found in communications may result in disciplinary action up to and including termination of employment.
4. Proof-read your emails before sending them. Use the spell check function to ensure that the message is free of unnecessary spelling errors. Where an email includes grammatical or spelling errors or is inaccurate, we risk the chance of being viewed as unprofessional and may potentially lose business or disappoint our customers.
5. Use an appropriate and professional tone in the email messages. It is often very difficult to determine when a person is using humour, sarcasm, or irony in an email. Please note that emails that include humour may be misunderstood, and the effects may negatively impact our business.
6. At all times, please avoid the use of the “All Caps” function, as messages sent using all CAPITALS is the e-mail version of yelling, and may be taken as offensive.
7. Keep messages short, simple, clear and concise.
8. Remember that when you send an email, it creates a permanent electronic record. Whatever is written in your email will be on the record for all time. Ensure that all messages sent are appropriate, and accurate in their content.
9. While it's common to use short-hand for personal notes, it is unacceptable for business communication. Standard abbreviations (including: e.g., Mrs., Mr., etc.) will continue to be acceptable, however, the use of excessive or colloquial abbreviations (LOL, ROFL, TTYL, BRB, etc.) is unacceptable.
10. Ensure that all messages are sent only to the intended recipients.
11. Emails that contain financial information (quotes, costs, etc.) must be checked for accuracy.

12. Under no circumstances should confidential business information be sent out to any third party using email, without prior written authorization from management.
13. Ensure that all passwords are maintained securely, and change your password a minimum of once each month. Do not share your password with others, including colleagues. Passwords should include letters, numbers and special characters.
14. Alert management immediately of any breach in email security.
15. Check your email frequently. If any emails are missed, there is the potential for lost business, miscommunications, or failure to complete required job duties.
16. Mark spam messages appropriately and file them in the spam folder.
17. Never reply to spam messages.
18. Open attachments only from known senders.
19. If the volume of spam becomes unmanageable, contact the department or individual in charge of managing the facility's information technology in order that they may address the issue.
20. Archive all messages that are older than three months.

Any email sent from a company computer and company email address is considered the property of the employer. As such, management reserves the right to review all emails received and/or sent by their employees.

6.7 Social Media Policy

Intent

This document is designed to provide employees with guidelines regarding the appropriate use of the organization's social media pages and social media in general.

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 social media. 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

The employer utilizes various social media applications, such as Facebook, Twitter. LinkedIn and Instagram as a means of communicating company information, including promotions and other marketing initiatives to customers, potential customers and the communities that it operates within. Use of social media is subject to strict guidelines to ensure confidential and proprietary information remains protected and that communication via online media is appropriate and consistent with the values and mission of the company.

The following guidelines shall govern employee use of social media applications.

1. Do not disclose confidential or proprietary information on any company-operated social media page. Disclosure of confidential or proprietary information without prior authorization may result in immediate termination.
2. Employees will be held responsible for what they write or post on any company social media page. Inflammatory comments, disparaging remarks, or negative/inappropriate language or posts will result in disciplinary action up to and including termination.
3. Employees are directed not to engage in discussions regarding competitors in the industry, legal issues in which the company is involved, or government issues related to the company and our industry without prior approval from management.
4. Respect copyrights. Do not post text, images or video that were created by someone else without proper authorization. Direct questions about copyright law and/or usage of certain media to management.
5. Social media is not a substitute for inter-company communications. Important information should be transmitted within normal company communication channels, not on Facebook etc.
6. Social media is not a substitute for customer service. Please refer customers to the appropriate phone number and department instead of handling inquiries entirely through social media platforms.
7. If an employee discovers any group(s) that users have formed to discuss the company, its products, or services, please bring them to the attention of management.
8. If you have questions about how to respond to a specific post or group, discuss the issue with management prior to replying.

9. Use good judgment when posting photos from company events. Notify any employees who are in photos so that they may approve the posting of the photos.

10. Always adopt a positive attitude when responding to comments on the company's pages or applications, or comments about the company in general.
11. Only designated employees are eligible to post on the company social media platforms and respond to comments.

6.8 Network Security Policy

Intent

The employer strives to protect company computer networks from both internal and external threats to their integrity, and to preserve confidentiality. This policy has been adopted to ensure that every reasonable effort has been taken to prevent and mitigate the effects of serious risks and potential costs associated with threats to networks and network resources.

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 network security. 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

Threats to the security of computer networks pose a significant risk to the organization's ability to carry out its operations.

The network operates at the continual risk of intrusions such as, but not limited to, theft of confidential information, the spread of viruses and malware and other activities designed to damage and or destroy network functionality.

The employer has an obligation to exercise due diligence to protect sensitive data and may face legal action if personal and or confidential information is disclosed.

Network Users:

- Comply with all employer policies.
- Comply with all protocols regarding connection to company networks.

IT Department or Representative:

- Act as the final authority on all network security related activities.
- Oversee any investigations into alleged network security issues.
- Develop protocols for tracking suspected network intrusions and test these methods for validity.
- Work with appropriate authorities towards the identification and prosecution of groups and individuals involved in activities in violation of company policy and the law.
- Post security alerts, network usage best practices and any other information required to protect the network.
- Monitor all network traffic to detect any unauthorized activity, attempts at intrusion and compromised hardware in compliance with privacy and confidentiality policies.
- Resolve any identified potential or actual problems in collaboration with appropriate managers.
- Regularly test the network for vulnerabilities using appropriate tools.
- Report any ongoing concerns to management.

- Undertake any necessary upgrades and or repairs to the network to maintain network security.
- Produce quarterly reports of all security related activities, concerns and or problems identified and resolved.
- IT Department or representative contact information should be posted in all departments.