I.T. & Computer Use Policy No. 14.143

District of Lake Country
10150 Bottom Wood Lake Road
Lake Country, BC V4V 2M1
t: 250-766-5650 f: 250-766-0116
lakecountry.bc.ca

Date

The following policy replaces IT & Computer Use Policy No. 13.128 and was approved as an Administrative Policy on November 27, 2014.

Purpose

The District of Lake Country ("District") provides Council members, permanent and select casual employees with Internet access and electronic communications services as required for the performance and fulfillment of job responsibilities.

Employees must understand that this access is for the purpose of increasing productivity and not for non-business activities. Users must also understand that any connection to the Internet offers an opportunity for non-authorized users to view or access corporate information, therefore it is important that all connections be secure, controlled and monitored.

To this end, users should have no expectation of privacy while using company-owned or company-leased equipment. Information passing through or stored on company equipment can be monitored. Users should also understand that the District maintains the right to monitor and review Internet use and e-mail communications sent or received by users.

The use of electronic devices at Council meetings and other District meetings will mean a reduction in the amount of paper used by the District. In 2009, the District committed to a paperless strategy and adopted the use of tablets/computers as a method by which the District agendas and other District information would be accessed by Council.

Policy

1.1 NETWORK ACCESS AND SECURITY

Network access is granted by Technology Support upon authorization from the District Chief Financial Officer (CFO) for staff and Chief Administrative Officer (CAO) for Council. A user:

- Must access the company computing and network resources using his/her assigned user ID and secret password.
- Must be responsible for selecting and protecting his/her secret password (not choosing an easy to guess password, not sharing passwords, keeping passwords hidden etc.)
- Must be responsible for all activity conducted under his/her use account
- Employees must notify Technology Support or the CFO immediately upon suspicion of unauthorized activity.

- Council must notify the CAO if they believe the security of their electronic device has been compromised.
- Must utilize the auto-lock feature, set to fifteen minutes or less, with a secure password to prevent unauthorized use.
- Must ensure that the device remains secure at all times and that the password and/or device is not shared with any other party.

1.2 NETWORK AND APPLICATION INTEGRITY

Users are responsible to maintain and protect the District's network, computing equipment, devices and passwords. A user must:

- Take appropriate precautions to store and protect confidential data, authentication credentials, PINS and passwords.
- Take reasonable physical security measures to safeguard computer equipment and devices (storing laptops in locked cabinet, enabling password protection on laptops/workstations and timeout for inactivity etc.)
- Ensure that computer software and equipment devices meet minimum system requirements where Technology Support is not responsible for software and/or equipment installation.
- Restrict his/her activities to what they are expressly authorized to do.
- Non-authorized devices (pcs, laptops, phones, printers, etc.) are not permitted.
- Addition of network devices such as hubs, switches, wireless access points, routers, etc. must be authorized by Technology Support.
- Moving of desktop computer and related equipment must be done with authorization of Technology Support/Financial Analyst/CFO.

1.3 EMPLOYEE PERSONAL USE

The District's Electronic Communication Resources are a corporate asset which must be used primarily for legitimate business purposes. Personal use is not forbidden, but such use:

- Must be limited and not affect work performance and normal business activities;
- Must not directly or indirectly interfere with the District's operation of Electronic Communication Resources; and
- Must not compromise the security or reputation of the District.

Employee personal use does not include uses requiring substantial expenditures of time, uses for profit or uses that would otherwise violate company policy with regard to employee time commitments or company equipment.

Permitted use by employees is at the discretion of Management and Technology Support and may change at any time.

1.4 COUNCIL PERSONAL USE

It is expected that there may be some reasonable personal use on the device, such as emails, calendar appointments and other applications. Personal files should be kept separate from District files. It is recommended that users delete any unnecessary notes from the device once they are no longer required. Exceptions are to be approved by CAO.

1.5 BREAKAGE AND LOST OR STOLEN DEVICES

Council members and staff will be responsible to ensure the device remains in their custody and is not handled or accessed by any unauthorized person.

In the event that an electronic device is lost or stolen the Council member will report the loss or theft to the CAO and employees will report this loss or theft to the CFO as soon as is practical. The District reserves the right to disable or wipe the device.

The District will arrange for repairs or replacement for damages incurred while operating the device for District business. If the device is damaged during personal use, the District will repair or replace the device at the staff/Council member's cost.

1.6 INTERNET AND ELECTRONIC MAIL

The District provides Internet connection and email capabilities to approved users. The company follows industry standard practices regarding virus protection, firewall security and anti-spam; and enables authentication and encryption tools. Internet and Electronic mail include many forms of communication including but not limited to Instant Messaging, Facebook, Twitter, blogs, forum posts, voice chat and Skype. An Internet and email user must:

- Waive his/her right to privacy and be aware that his/her activities may be monitored.
- Use only his/her assigned user ID and email address.
- Use industry best practices including: not opening and deleting email or attachments that look suspicious and using acceptable etiquette and language.
- Restrict activities to "business related" when subscribing to newsletters or mailing lists, using blogs, chat rooms or newsgroups.
- Refrain from emailing "non-business related" communication including but not limited to chain letters, charitable solicitations, political campaign material, religious work and transmission of objectionable material or business schemes for personal gain. Personal communications may be posted on the employee Intranet under the section "Non-Work Related Announcements." This section will be monitored so please use discretion when attaching personal posts.
- Notify Technology Support immediately upon receipt of excessive spam, threatening or objectionable communications.

1.7 SOFTWARE CODE OF ETHICS

The District respects all computer software copyrights and adheres to the terms of all software licence agreements to which the company is a party. A user must:

- Use software only in accordance with its licence agreement.
- Obtain CFO approval prior to purchasing, loading, downloading, installing, distributing any software, shareware, MP3 files, etc.
- Maintain purchasing and licensing documents that provide "proof of ownership" for all software where Technology Support is not responsible for software installation.
- Notify Technology Support immediately upon suspicion of unlicensed software being used within the company. All software must be purchased or authorized by Technology Support/CFO.
- Copy and securely store personal computer software used within the company.

1.8 APPLICATIONS ("apps")

The ability to download and install third-party applications (hereafter referred to as "apps") onto devices is pervasive. Many of these apps provide true business value, while other apps are purely for entertainment. Some apps are free, while others incur additional charges to the user. The District will not censor or regulate downloading and installation of additional apps onto District-issued devices. As such, it is the responsibility of the user to:

- Ensure apps downloaded, installed and used on devices are consistent with this and all applicable policies and any relevant government legislation.
- Ensure additional memory, apps or features above those deemed necessary by the District for normal business use are acquired at the user's expense.

1.9 INFORMATION STORAGE

- Unless authorized, store all information in the appropriate location (on servers) where it can be properly managed.
- No storing information on local PC.
- No storing information on non-District servers (cloud storage, file sharing sites, etc.)
- No copying information onto removable drives/taking home/emailing unless authorized through Technology Support.
- Store information in a manner that makes it easy for other users to find and use:
    - sensible location
    - sensible file name
    - no password protection on files
    - ensure proper version control:
        - Ensure old versions of documents are archived or otherwise managed so everybody is using the same file version.

1.10 PROHIBITED ACTIVITIES

A user must not engage in any unauthorized or illegal activity under local, provincial, federal or international law or in violation of company policy including but not limited to: unauthorized/illegal use or access to computer systems, networks and files, copyright or infringement violations and harassment activities.

1.11 RESPONSIBILITIES

Users are responsible for:

- Honouring acceptable use policies of networks accessed through the District's Internet and e-mail services;
- Abiding by existing federal, provincial and local telecommunications and networking laws and regulations;
- Following copyright laws regarding protected commercial software or intellectual property;
- Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of the District's network resources; and
- Not overloading networks with excessive data or wasting the District's other technical resources.

1.13 STAFF VIOLATIONS

Violations will be reviewed on a case-by-case basis. If it is determined that a user has violated one or more of the above use regulations, that user will receive progressive discipline from his or her supervisor and his or her future use will be closely monitored. If a gross violation has occurred, management will take immediate action. Such action may result in losing Internet and/or e-mail privileges, or more severe discipline, up to and including termination.

Original signed by Alberto De Feo	*27 November 2014*
Alberto De Feo, CAO	Date

I have read and understood **IT and Computer Use Policy No. 143**.

Name (print)	Signature	Date