**REGIONAL DISTRICT OF OKANAGAN-SIMILKAMEEN**
**BOARD POLICY**

**POLICY:** Information Systems Use and Social Media Policy

**AUTHORITY:** Board Resolution dated June 18, 2015.

**AMENDED:** Board Resolution dated May 19, 2016[1].

## POLICY STATEMENT

The use of computers and social media in both a personal and professional setting is now, and will more so become critical to the success of the Regional District of Okanagan-Similkameen (RDOS). To maintain the credibility and trust of our citizens, it is important that our employees, volunteers and elected officials be accountable for maintaining high standards of ethical conduct in their use of company property.

## PURPOSE

1. To establish corporate practice and provide guidance around acceptable and appropriate usage of:
    a. computers owned by the RDOS and provided to employees, volunteers and elected officials for work purposes; and,
    b. work related Social Media
2. To set out the means to correct unethical conduct;

## DEFINITIONS (IF REQUIRED)

**"Computer"** is defined as Computer hardware and ancillary devices (including but not limited to desktop and laptop workstations, mobile or "smart" phones, tablet computers, PDA's, and portable USB Flash drives photocopiers, printers, fax machines and the telephone system) as well as the software and data contained on them.

**"Information Systems"** include (but are not limited to) Computers, network infrastructure, servers, internet, remote access, corporate software (including but not limited to email, Electronic Document Management Software, Financial and GIS) and databases.

**"Social Media"** is defined as any group of internet based applications that allow the creation and exchange of user-generated content (including but not limited to Facebook and Twitter).

**"Illegal activity"** is an act committed in violation of the law (including but not limited to downloading copyright or pirated songs or videos and hacking into other computer systems).

## RESPONSIBILITIES

1. The Board of Directors shall:
    a. make such revisions, additions or deletions to the Policy as may be required.
    b. investigate allegations and inquiries relating to unethical conduct by elected officials and the CAO and take appropriate action.

2. The Chief Administrative Officer shall:
    a. make such revisions, additions or deletions to the Policy as may be required by law.
    b. investigate allegations and inquiries relating to unethical conduct by employees and volunteers and take appropriate action.
    c. ensure the administrative controls referred to in the Code of Conduct are in place.

3. Information Services Department shall:
    a. maintain overall security and integrity of the Information Systems.

4. Managers shall:
    a. ensure that each employee in their Department is familiar with this policy.

5. User's shall:
    a. comply with this policy and any related procedural documents that may be issued.
    b. not use the Information Systems for an activity that could expose the RDOS, themselves, or colleagues to potential criminal, ethical or any legal proceedings.
    c. take reasonable steps to not compromise the performance and/or affect the integrity of the Information Systems.
    d. follow security measures and restrictions that are in place.
    e. report to the Information Services Department if something potentially negative happens, or anything suspicious is noticed in regards to the Information Systems.

**PROCEDURES**

This Procedure is broken down into four specific areas:

1. General Computer use guidelines for employees and Elected Officials on RDOS Computers.
2. RDOS Social Media internal operational guidelines.
3. Internal guidelines for public interaction with Social Media sites and key components to keep in mind.
4. General guidelines and summary.

## 1. *General Computer Use Guidelines for Employees, Volunteers and Elected Officials on RDOS Computers.*

1.1 The RDOS recognizes there are times when company Computers may be used (i.e. email, web surfing, use of audio/visual programs/software, Social Media sites, phones) for personal use. However using Computers for personal use must not affect the productivity, disrupt the system and/or harm the RDOS's reputation.

1.2 All Computers are to have a login password set and a Computer lockout after a period of idle activity.

1.3[1] Login information (including PIN or Personal Identification Number for RDOS phones) is to be protected and not shared with anyone. The exception being for IT related troubleshooting purposes only.

1.4 Report lost/stolen Computers to the Information Services Department as soon as possible.

1.5 Downloading of large personal use programs/files/software is monitored by IS Department for bandwidth usage and security issues, and subsequent information may be brought to the users attention, or their respective supervisor. Users unsure of bandwidth allocation/usage for specific downloads/programs should consult the IS Department beforehand.

1.6 Downloading and/or viewing illegal material or participating in illegal activity on RDOS Computers is not permitted. Illegal activity conducted on RDOS Computers and/or portable/handheld devices will be dealt with through respective legal and labour relations means.

1.7 Downloading and/or viewing of pornographic material on the internet, or through email, is not permitted, and any user caught downloading/viewing pornographic material will face disciplinary action.

1.8 Installation of non-work-related programs/software or "apps" should be approved by the IS Department. Installed non work-related programs/software is subject to removal by IS Department.

1.9 Do not intentionally expose the Information Systems to viruses, spyware or other security threats. Make every effort to avoid risky websites, programs, emails, attachments, etc. If you are not sure what something is, please consult the IS Department.

1.10 If there is a need for data to be taken out of the corporate environment or work related personal/non-public data to be stored on a RDOS portable storage device (including but not limited to USB flash drives, SD cards, USB hard drives), then the RDOS portable storage device must be encrypted with appropriate password protection.

1.11 Use of RDOS Computers for private enterprise is not permitted unless authorized by the CAO.

1.12 Use of cloud servers outside Canada (including but are not limited to Dropbox, iCloud, Google Drive, SkyDrive) is discouraged. Downloading of documents/files from these sites is permitted but any outgoing documents/files should be managed on the RDOS cloud file share (i.e., ownCloud) or the RDOS FTP (File Transfer Protocol) site. Please contact the IS Department if you are unsure on how you should be using cloud services.

1.13 If a user requests to connect their personal device to the corporate e-mail system, and such action is approved by their department manager and the IS Department, the user must sign the Personal Device Usage Agreement.

1.14[1] Staff and Elected Officials are permitted to share their calendar with other staff and Elected Officials at their discretion. Because of the sensitive nature sometimes found in email, sharing of email mailboxes is only to be done if an employee has left the organization, if it is a "resource" type mailbox (i.e. info@rdos.bc.ca) or rarely and at the Managers discretion if the employee is unavailable (i.e. sick or on holiday) and access is required of the mailbox.

1.15 Some corporate web based applications including but not limited to OWA (Outlook Web Access), RDP (Remote Desktop Protocol) and EDMS (Electronic Document Management System) allow downloading of documents to local computers outside the RDOS network. Any downloading of documents should only be done on a temporary basis and corporate documents are not to be stored on remote personal computers.

## 2 *RDOS Social Media Internal Operational Guidelines.*

2.1 The RDOS has approved Social Media accounts (example: Facebook, Twitter, YouTube) which are operated internally by staff designated by the CAO or a CAO-approved designate. Any new Social Media sites must be approved by the CAO.

2.2 The RDOS's Social Media sites are public forums and platforms for information release which can include the following: utilities advisories, emergency services, public hearings, bylaw announcements, information releases, photos, maps, reports and any other information deemed pertinent and approved for public viewing by designated staff.

2.3 Until there is a dedicated resource to monitor Social Media sites, the ability for the public to add posts, general requests or comments to the RDOS Social Media sites will be disabled whenever possible.

## 3. *Internal Guidelines for Public Interaction With Social Media Sites and Key Components to Keep In Mind.*

3.1 RDOS users are not recommended to directly link their personal Social Media site profile to the RDOS's approved Social Media sites, unless they feel confident about their knowledge of the specific Social Media platform. Linking a personal site to an employer's site forms a professional connection via Social Media, thus an exchange of information may also take place and staff should take a proactive approach and educate themselves about applicable privacy settings beforehand.

3.2 Users are not permitted to use company email as login accounts for personal Social Media sites.

3.3 Users are required to comply with the code of conduct when answering questions or posting/linking information to other Social Media sites on RDOS related business.

## 4. *General guidelines and summary*

4.1 Users should be aware that RDOS Computers can be monitored internally, and made public through a *Freedom of Information and Protection of Privacy Act* request. Access to these devices may be requested by the Head of FOI at any time.

4.2 Collection of personal information through monitoring applications will be in accordance with *Freedom of Information and Protection of Privacy Act* legislation.

4.3 The RDOS reserves the right to recover costs due to inappropriate use of company property which includes Computers and Portable Devices.

4.4 Users assume responsibility and risk by using personally owned devices in the corporate environment.

**RELATED POLICIES**

Electronic Mobile Communication Device Policy