qathet REGIONAL DISTRICT

SECTION 1 **CORPORATE POLICIES**

POLICY **1.18**

SUBJECT **COMPUTER AND NETWORK SYSTEMS POLICY**

ADOPTED **DECEMBER 6, 2023**

---

1. POLICY STATEMENT

qathet Regional District (qRD) provides Users with access to Computer and Network Systems to support activities directly related to the performance of their duties in service of the qRD.

To maintain the functionality and security of qRD's Computer and Network Systems, Users must follow the guidelines laid out in this policy, practice sound and prudent judgment and maintain high standards of ethical conduct in their use of qRD's Computer and Network Systems.

2. DEFINITIONS

"**Computer and Network Systems**" means:

- Electronic hardware and equipment owned or leased by the qRD including but not limited to desktops, laptops, tablets, servers and telephones (including analog, IP, and cellular), scanners, printers and fax machines and other peripheral devices and removable media and data storage devices (such as USB memory sticks, CDs, etc.);
- Computer software, applications, accounts and services owned, leased or subscribed to by the qRD, such as email, network file services, records management systems, financial software, and any qRD-managed social media accounts or cloud services, including third party provided services; and
- Transmission methods and services financed by the qRD, including wired, wireless and cellular services, whether accessed from within the qRD's premises or elsewhere.

The definition of Computer and Network Systems does not cover use of qRD-owned and managed products or services by customers or other third parties, such as viewing the qRD website.

"**Elected Officials**" means the individual members of the qRD Board of Directors.

"**Non-Public Information**" means information that is confidential or is exempt or is potentially exempt from disclosure under the *Freedom of Information and Protection of Privacy Act* (the FOIPPA).

"**Users**" includes everyone who has access to any of qRD's Computer and Network Systems, including but not limited to employees, fire department members and Elected Officials. It may also include those who may be engaged by the qRD to provide a service, including contractors, agencies, consultants, volunteers and business partners.

3. PURPOSE

To establish a policy governing the ownership, monitoring, support, security, and acceptable use of qRD's Computer and Network Systems.

4. SCOPE

This policy applies to all Users and to all qRD Computer and Network Systems.

Some aspects of this policy affect areas governed by local legislation in certain jurisdictions (e.g., employee privacy laws). In such cases, the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction.

5. GUIDELINES

5.1 Ownership

a. Computer and Network Systems will be provided to Users to support activities directly related to the performance of their duties in service of the qRD. All Computer and Network Systems are the property of the qRD and will be returned to the qRD once a User is no longer working for or with the qRD or in their role as an Elected Official.

b. All documents, files, electronic communications (including qRD and personal emails) and web content systems created on, generated by or transmitted through the Computer and Network Systems are the property of the qRD, including that marked personal, private or confidential and are subject to the FOIPPA.

5.2 Monitoring

a. The qRD reserves the right to monitor and audit the use of its Computer and Network Systems. This includes, but is not limited to, reviewing user activities, network traffic, software usage, and data stored on the Computer and Network Systems. By using qRD's Computer and Network Systems, Users acknowledge and consent to the monitoring and auditing activities conducted by the qRD to ensure compliance with policies, security standards, and legal regulations.

b. Monitoring and auditing activities may be performed on a regular basis or in response to specific incidents or concerns.

5.3 Support

a. The qRD Technical Services Department or a designated contractor will perform required maintenance on Computer and Network Systems. Electronic hardware and equipment owned by the qRD should not be taken for service to anyone other than the qRD Technical Services Department without the written authorization of the Technical Services Department.

b. Users of qRD-issued desktops and laptops that are not directly connected to qRD's network (e.g., Elected Officials and fire departments) will ensure that they turn on these devices and connect them to the internet at least bi-weekly to facilitate the automated update of the operating system or other installed software/applications.

c. A qRD-issued desktop, laptop or other device that is not directly connected to qRD's network will not be backed up by the qRD, with the exception of Users' email. If a qRD-issued desktop, laptop or other device is backed up by a User onto a separate removable media and data storage device, the media and data storage device should be newly acquired and used exclusively for this backup purpose. The removable media and data storage device must be protected to the same extent as the User is protecting all Computer and Network Systems.

d. The qRD Technical Services Department will provide support for the use of Computer and Network Systems for any activity or business performed in service of the qRD.

e. If Computer and Network Systems are damaged as a result of any activity or business not performed in service of the qRD, the cost to repair or replace the Computer and Network Systems may be borne by the User.

5.4 Security

a. Users are responsible for the protection of the Computer and Network Systems from access by anyone other than themselves.

b. Passwords should not be shared with anyone. The only exceptions being for IT related troubleshooting purposes by the Technical Services Department or a designated contractor or for a FOIPPA compliant review of the Computer and Network Systems by the Corporate Officer. If a device or account password is written down, it should not be attached to the device or stored in a way that identifies it as being a password for the device or associated user accounts.

c. Users may not download or install software or applications without first obtaining written authorization from the Technical Services Department to ensure security and compatibility with Computer and Network Systems and that sufficient resources are in place to support the software.

d. The storage and/or transfer of Non-Public Information to servers or other devices located outside Canada must be in compliance with the FOIPPA.

e. Users must actively protect Non-Public Information by ensuring that it is not viewable or accessible by unauthorized persons and should observe access and privacy provisions of the FOIPPA.

f. Users are responsible for the physical security of their qRD-issued portable devices (laptops, tablets, cellular phones, smartphones, etc.) and must ensure that these devices are not handled or accessed by unauthorized persons. Such portable devices must not be left unattended in any public setting.

g. All qRD-issued portable devices are to have a login passcode/PIN code set and they must be set to lock the screen after a period of idle activity.

h. Any Computer or Network Systems that are suspected lost or stolen must be reported to the Technical Services Department immediately.

i. Users must report to the Technical Services Department if they suspect an action has been taken that may cause a compromise to Computer and Network Systems or a breach of Non-Public Information or simply, if something potentially negative or suspicious is noticed. Indications of a compromised system might include unexplained lockouts, content or activity; unexpected programs running; data appearing to be missing or changed; and increased frequency of system crashes.

j. Users must participate in cybersecurity training programs as directed by the Chief Administrative Officer.

5.5 Acceptable Use

a. Users are to use Computer and Network Systems to support activities directly related to the performance of their duties in service of the qRD.

b. Computer and Network Systems shall be used in a manner that is ethical and professional. Such conduct demonstrates respect for intellectual property, ownership of qRD information, and network and information technology asset security.

c. Users who are issued qRD owned cellular phones or smartphones or are approved to use a personal cellular phone or smartphone for the performance of their duties in service of the qRD will act in accordance with current laws regarding the use of such devices when operating powered vehicles or equipment.

d. Limited occasional or incidental personal use of qRD's Computer and Network Systems is acceptable, subject to the following conditions:

   i. Usage is brief and its volume, frequency or both does not disrupt qRD business, disrupt other Users, or interfere with any employee productivity, work duties, or responsibilities.

   ii. Usage does not compromise the security or integrity of qRD's Computer and Network Systems or other services, assets or qRD information, particularly Non-Public Information.

   iii. Usage does not result in a financial cost of more than $1 to the qRD, e.g., making personal long distance calls on a qRD office phone or qRD owned cellular phone or smartphone, making ten (10) photocopies or more on qRD owned photo copiers, etc. In the event that personal usage results in a financial cost to the qRD above $1, the User will reimburse the qRD. These costs may be overridden in accordance with the provisions of the qRD Fees and Charges Bylaw.

   iv. Usage complies with this policy, with all other qRD policies and with all relevant legislation, including FOIPPA.

5.6 Unacceptable Use

This list of activities is provided as examples of unacceptable use; however, it is not exhaustive.

a. Intentionally exposing Computer and Network Systems to viruses, spyware or other security threats.

b. Engaging in illegal activities. This would include any act committed in violation of the law including but not limited to downloading copyright or pirated material onto qRD's Computer and Network Systems and hacking into other computer systems.

c. Engaging in unethical activities. This would include, but is not limited to accessing, viewing, creating, posting, sending, or downloading discriminatory, violent, threatening, intimidating, harassing, or pornographic materials on Computer and Network Systems.

d. Intentionally accessing confidential qRD information and Non-Public Information on Computer and Network Systems that is not required for the User's duties.

e. Directly connecting non-qRD computing devices such as smartphones, tablets, laptops, removable media and data storage devices and other devices to Computer and Network Systems without the written authorization of the Technical Services Department.

f. Using Computer and Network Systems for private enterprise.

g. Downloading, uploading, backing up or storing Non-Public Information on a personal device outside of Remote Desktop or on a cloud file share (iCloud, Dropbox, etc.). Examples of this practice include but are not

limited to opening qRD's in-camera agendas or meeting minutes or other Non-Public Information on non qRD-issued devices or personal devices outside of Remote Desktop as the act of opening one of these documents may result in its download to a non qRD-issued device or personal device.

h. Entering or copying Non-Public Information into an Artificial Intelligence (AI) language model is unacceptable. These AI language models use data from user inputs/queries to process and generate responses and there is no guarantee that the information that is entered will remain private or confidential. There is a risk that input data could be exposed or misused.

i. Connecting a non qRD-issued device or personal device to qRD's corporate email system is unacceptable unless done in compliance with 1.17 Electronic Mobile Communication Device Policy. This is not to be confused with using Outlook on the Web or Remote Desktop on a personal device to view qRD's corporate email system.

6. RESPONSIBILITY/AUTHORITY TO ACT

6.1 Board of Directors

a. Make such revisions, additions or deletions to this policy as may be required.

b. Review reports on claims of non-compliance of Elected Officials with this policy and take appropriate action.

6.2 Chief Administrative Officer

a. Promote awareness and understanding of this policy.

b. Direct and support efforts to educate Users around the appropriate use of Computer and Network Systems.

6.3 Corporate Officer

a. Promote awareness and understanding of this policy.

b. Receive reports on claims of non-compliance with this policy and assist the Technical Services Department with investigations into such claims.

c. Report findings of investigations into claims of non-compliance with this policy by Elected Officials to the Board of Directors.

d. Report findings of investigations into claims of non-compliance with this policy by Users other than Elected Officials to the User's manager (or in the case of the User being a fire department member, to the Manager of Emergency Services) along with advice on the appropriate action to take to address the act of non-compliance.

e. Work with the Technical Services Department to take all necessary steps to protect the qRD and its Computer and Network Systems and to mitigate risks to the qRD of non-compliance with this policy. Steps may include, but are not limited to, removing a User's access to Computer and Network

Systems until findings of any investigation into claims of non-compliance with this policy are resolved and appropriate action is taken.

6.4 Technical Services Department

a. Responsible for the overall administration and maintenance of qRD's Computer and Network Systems.

b. Provide Computer and Network Systems' support to Users for any qRD-related activity or business.

c. Provide guidance to Users on the interpretation of this policy.

d. Receive reports of Computer and Network Systems' loss, theft, or suspected compromise and take appropriate action in accordance with the qRD's Cyber Security Incident Response Plan.

e. Assist the Corporate Officer with investigations into claims of non-compliance with this policy.

f. Work with the Corporate Officer to take all necessary steps to protect the qRD and its Computer and Network Systems and to mitigate risks to the qRD of non-compliance with this policy. Steps may include, but are not limited to, removing a User's access to applications or at-risk data or to all Computer and Network Systems until findings of any investigation into claims of non-compliance with this policy are resolved and appropriate action is taken.

6.5 Managers

a. Ensure that Users under their direct supervision, hired contractors and other authorized Users, are aware of, and comply with this policy.

b. Report any suspected acts of non-compliance with this policy to the Corporate Officer.

c. Work with the Corporate Officer to take appropriate action against acts of non-compliance with this policy by Users under their direct supervision, hired contractors and other authorized Users.

6.6 Users

a. Comply with this and related policies and acts.

b. Report any suspected acts of non-compliance with this policy to the Corporate Officer.

7. POLICY REVIEW DATE

This policy will be reviewed periodically.

8. RELATED POLICIES AND ACTS

- 1.17 Electronic Mobile Communication Device Policy
- *Freedom of Information and Protection of Privacy Act*