



qathet

REGIONAL DISTRICT

SECTION 1	CORPORATE POLICIES
POLICY	1.17
SUBJECT	ELECTRONIC MOBILE COMMUNICATION DEVICE POLICY
ADOPTED	DECEMBER 6, 2023

1. POLICY STATEMENT

qathet Regional District (qRD) provides Users with access to Electronic Mobile Communication Devices to support activities directly related to the performance of their duties in service of the qRD.

Employees, Elected Officials, fire department members or any other User may request to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system only in accordance with the guidelines of this policy.

To maintain the security of Electronic Mobile Communication Devices, 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 Electronic Mobile Communication Devices.

2. DEFINITIONS

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

"Electronic Mobile Communication Device" means a computer with cellular data access, a cellular phone, or a smartphone.

"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" means everyone who has access to any qRD-owned Electronic Mobile Communication Device, including but not limited to authorized employees, fire department members, Elected Officials, contractors and volunteers. It also means those who have been authorized to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system.

"Usage Plan" means a subscription plan and associated options negotiated by the device owner with external vendors to provide wireless cellular service and data connectivity on wireless devices, cellular phones, and smartphones. Usage plans

prescribe billing rates for minutes, long-distance charges, text messaging, and data charges.

3. PURPOSE

To establish a policy governing the provision and administration of qRD-owned Electronic Mobile Communication Devices and the guidelines by which a person may use a personal Electronic Mobile Communication Device in service of the qRD.

4. SCOPE

This policy applies to all Users, to all qRD-owned Electronic Mobile Communication Devices and to all personal Electronic Mobile Communication Devices that have been authorized by the Chief Administrative Officer (CAO) to be in service to the qRD and/or to connect to qRD's corporate email system.

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.

Exceptions to this policy may be made on a case-by-case basis where extenuating circumstances exist, as approved by the CAO.

5. GUIDELINES

5.1 Eligibility

The issuance of a qRD-owned Electronic Mobile Communication Device to a User or the use of a personal Electronic Mobile Communication Device in service of the qRD and/or to be connected to qRD's corporate email system must be approved by the CAO. At the discretion of the CAO, criteria for eligibility includes but is not limited to:

- a. User is an Elected Official.
- b. User is a fire chief or deputy chief for one of the qRD's volunteer fire departments.
- c. User requires for job related safety.
- d. User spends time working alone and is required to check in on a regular basis.
- e. User requires for emergency or on-call contact purposes.
- f. User requires for "field to field" or "field to office" communications and/or where alternative communication devices (radios, etc.) are ineffective.
- g. User requires when the device is used to monitor critical equipment.
- h. User requires due to considerable time spent out of office with requirement to communicate with staff and/or public and to manage email in order to ensure uninterrupted customer service.
- i. User requires for operational efficiency.

5.2 Supply, Replacement and Disposal of qRD-owned Electronic Mobile Communications Devices

- a. Any employee wishing to be issued a qRD-owned Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must submit their request to their manager who will forward the request to the Technical Services Department. Technical Services Department staff will consult with, and obtain approval from the CAO.
- b. Any Elected Official wishing to be issued a qRD-owned Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must submit their request to the Technical Services Department. Technical Services Department staff will consult with, and obtain approval from the CAO.
- c. Any fire department chief or deputy wishing to be issued a qRD-owned Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must submit their request to the Manager of Emergency Services who will forward the request to the Technical Services Department. Technical Services Department staff will consult with, and obtain approval from the CAO.
- d. qRD's Technical Services Department staff will work with the User to identify and supply an Electronic Mobile Communication Device and associated Usage Plan that allows the User to perform their duties in service of the qRD.
- e. qRD's Technical Services Department staff will inform Users of details related to the Usage Plan including, but not limited to usage limits and travel roaming options/considerations.
- f. qRD's Technical Services Department will assist Users in configuring basic connectivity, including connecting the Electronic Mobile Communication Device to qRD's corporate email system.
- g. If a qRD-owned Electronic Mobile Communication Device needs to be replaced for reasons including, but not limited to damage, poor functionality or loss, the User will contact Technical Services Department staff who will work to replace the Electronic Mobile Communication Device at a reasonable cost to the qRD.
- h. qRD-owned Electronic Mobile Communication Devices which have been damaged and will not be replaced should be reported to Technical Services Department staff who will immediately stop the monthly Usage Plan.
- i. qRD-owned Electronic Mobile Communication Devices which are not going to be used for an extended period of time (more than one month) should be reported to Technical Services Department staff who may move the unit to a minimum monthly cost Usage Plan.

- j. Any qRD-owned Electronic Mobile Communication Device that is no longer being used must be returned to Technical Services Department staff who will retain the device and all of its content in accordance with the FOIPPA.

5.3 Security and Acceptable Use of qRD-owned Electronic Mobile Communication Devices

qRD-owned Electronic Mobile Communication Devices are part of qRD's Computer and Networking Systems as defined in Policy 1.18 Computer and Network Systems Policy. Therefore, the Guidelines identified in that policy must be followed when using a qRD-owned Electronic Mobile Communication Device.

5.4 Use of Personal Electronic Mobile Communication Devices

- a. Any employee wishing to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must submit their request to their manager who will forward the request to the Technical Services Department. Technical Services Department staff will consult with, and obtain approval from the CAO.
- b. Any Elected Official wishing to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must submit their request to the Technical Services Department. Technical Services Department staff will consult with, and obtain approval from the CAO.
- c. Any fire department chief or deputy wishing to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must submit their request to the Manager of Emergency Services who will forward the request to the Technical Services Department. Technical Services Department staff will consult with, and obtain approval from the CAO.
- d. Any User that has been authorized by the CAO to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must sign a Personal Electronic Mobile Communication Device Usage Agreement in the substantial form of Schedule A.
- e. No connection of a personal Electronic Mobile Communication Device to qRD's corporate email system is permitted unless authorized by qRD's CAO and until the owner of the personal Electronic Mobile Communication Device and the CAO have signed a Personal Electronic Mobile Communication Device Usage Agreement in the substantial form of Schedule A.

- f. A User, with the exception of an Elected Official, will be entitled to a monthly stipend for the use of their personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system, only if a Personal Electronic Mobile Communication Device Usage Agreement has been signed by the User and the CAO.

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. Approve the issuance of qRD-owned Electronic Mobile Communication Devices and approve the use of a personal Electronic Mobile Communication Device to be in service to the qRD and/or to connect to qRD's corporate email system.

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 advise 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 data 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 a qRD-owned Electronic Mobile Communication Device or removing access to qRD's corporate email system from a personal Electronic Mobile Communication Device in service to the qRD 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. Provide guidance to Users on the interpretation of this policy.
- b. Oversee and administer the selection, acquisition, maintenance, disposal and other related processes of qRD-owned Electronic Mobile Communication Devices and their associated Usage Plans.
- c. Ensure that Users of qRD-owned Electronic Mobile Communication Devices are informed of the details of their Usage Plans and any other relevant device information.
- d. Provide Electronic Mobile Communication Device support to Users for any qRD related activity or business.
- e. Bring requests for the issuance of a qRD-owned Electronic Mobile Communication Device or for the use of a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system to the CAO for approval.
- f. Perform all duties and responsibilities of qRD's Technical Services Department as identified in Section 4 of the Personal Electronic Mobile Communication Device Usage Agreement (Schedule A).
- g. Assist the Corporate Officer with investigations into claims of non-compliance with this policy.
- h. Work with the Corporate Officer to take all necessary steps to protect the qRD and its data 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 a qRD-owned Electronic Mobile Communication Device or removing access to qRD's corporate email system from a personal Electronic Mobile Communication Device in service to the qRD 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 are aware of, and comply with this policy.
- b. Bring requests for the issuance of a qRD-owned Electronic Mobile Communication Device or for the use of a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system to the Technical Services Department.
- c. Report any suspected acts of non-compliance with this policy to the Corporate Officer.
- d. 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

- 1.18 Computer and Network Systems Policy
- *Freedom of Information and Protection of Privacy Act*

1.17 Electronic Mobile Communication Device Policy

Schedule A

Personal Electronic Mobile Communication Device Usage Agreement

Any qathet Regional District employee, Elected Official, fire department chief or deputy, or any other person that has been authorized by qRD's Chief Administrative Officer (CAO) to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system must sign this Personal Electronic Mobile Communication Device Usage Agreement.

No connection of a personal Electronic Mobile Communication Device to qRD's corporate email system is permitted unless authorized by qRD's CAO and until the owner of the personal Electronic Mobile Communication Device and the CAO have signed this agreement.

1. DEFINITIONS

"Device Owner" means the employee, Elected Official, fire department chief or deputy, or any other person that has been authorized by the qRD's CAO to use a personal Electronic Mobile Communication Device in service of the qRD and/or to connect to qRD's corporate email system.

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

"Electronic Mobile Communication Device" means a computer with cellular data access, a cellular phone, or a smartphone.

"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).

"Usage Plan" means a subscription plan and associated options negotiated by the device owner with external vendors to provide wireless cellular service and data connectivity on wireless devices, cellular phones, and smartphones. Usage plans prescribe billing rates for minutes, long-distance charges, text messaging, and data charges.

2. TERMS

2.1 Ownership

- a. Any personal Electronic Mobile Communication Device remains the property of the Device Owner.
- b. Any qRD-related content, including that marked personal, private or confidential on a personal Electronic Mobile Communication Device is subject to the FOIPPA. Access to a personal Electronic Mobile Communication Device may be requested by the Corporate Officer at any time.

2.2 Personal Electronic Mobile Communication Device Restrictions

- a. Personal Electronic Mobile Communication Devices that are not set to receive regular operating system and applications updates will not be accepted for use.
- b. Rooted or jailbroken personal Electronic Mobile Communication Devices will not be accepted for use. This refers to devices where restrictions imposed by the manufacturer have been removed, giving a user access to the operating system to unlock features and install unauthorized software.
- c. Personal Electronic Mobile Communication Devices that are not protected by a PIN code, password, pattern lock or some form of biometric authentication and do not automatically lock after a period of inactivity will not be accepted for use.

2.3 Device Owner Responsibilities

- a. A Device Owner who is an employee of the qRD will not be expected to respond to work-related emails, calendar, text, etc. outside of working hours unless the Device Owner is on call or stand-by, or overtime has been approved by the Device Owner's manager.
- b. Device Owners must actively participate in qRD's cybersecurity training program.
- c. Device Owners must undergo an orientation training session with Technical Services Department staff prior to 'onboarding' a personal Electronic Mobile Communication Device to ensure that the device is being used properly in service of the qRD.
- d. Device Owners must not install pirated software or illegal content onto their personal Electronic Mobile Communication Device. Installation of apps from untrusted sources is forbidden.

- e. Device Owners are personally responsible and liable for maintaining their personal Electronic Mobile Communication Device and for paying for any hardware and support requirements, repair or replacement costs, and for their Usage Plan charges. All incurred charges are the responsibility of the Device Owner, regardless of whether such charges result from doing work in service of qRD or for personal use. This includes, but is not limited to, charges resulting from texts, data plan surcharges, long distance calls, navigation, application uses or from early termination fees.
- f. Device Owners are responsible for any costs derived from their personal Electronic Mobile Communications Device being compromised, regardless of whether the compromise was caused by its use in service of the qRD.
- g. Device Owners must contact the Manager of Financial Services immediately if they discontinue use of their personal Electronic Mobile Communications Device in service of the qRD so that stipend payments can be discontinued.
- h. Device Owners are responsible for ensuring that their Electronic Mobile Communication Device's operating system and applications are being automatically updated.
- i. Device Owners are responsible to ensure that any qRD-related content on their personal Electronic Mobile Communication Device is not accessed by anyone other than themselves. This includes a repair technician if the device is taken in for servicing or repair. In this event, the device should be disconnected from qRD's corporate email system and all qRD content should be removed prior to release of the device to the repair technician.
- j. Device Owners must notify Technical Services Department staff immediately in the event that a personal Electronic Mobile Communication Device is lost, stolen or suspected compromised. In any of these scenarios, the qRD Technical Services Department will change the account password to prevent additional email from being delivered to the device and will immediately execute a remote wipe of the device. The device will decide whether to wipe only qRD email, or all data (qRD IT does not control this). This wipe thus has the potential to delete other email accounts, personal photos, music, etc. from the device. Device Owners should perform backups of their personal data and information on a regular basis as a precaution.
- k. Device Owners will replace their Electronic Mobile Communication Device within seven (7) business days if it is lost, stolen, damaged, or otherwise becomes unusable in the service of the qRD.

- l. In the event that an Electronic Mobile Communication Device is being disposed of or repurposed by the Device Owner, the connection to qRD's corporate email system should be severed and all qRD content should be removed from the device prior to disposal or repurposing.
- m. In the event that the Device Owner is no longer employed by the qRD or working in service of the qRD, the connection to qRD's corporate email system should be severed and all qRD content should be removed from the device and any backup of the device.
- n. Device Owners agree to work with qRD's Technical Services Department staff to review the content on their personal Electronic Mobile Communication Device and any device backups to inspect for qRD content and to securely remove qRD content as deemed necessary by the Corporate Officer or Technical Services Department staff either during the relationship between the Device Owner with the qRD, or after. Possible scenarios include, but are not limited to Freedom of Information request investigations, termination of employment or working relationship with the qRD, if a data or policy breach is detected, a virus or similar threat to the security of qRD's data and technology infrastructure, or prior to the servicing or replacement of a personal Electronic Mobile Communication Device. If qRD data is to be removed, every attempt will be made to remove only qRD data, however there is no guarantee of this. A Device Owner will be afforded the opportunity to review the data being removed.
- o. If a Device Owner does not work with qRD's Technical Services Department staff in accordance with Section 3.n within one (1) week after a request is issued by the qRD, the Device Owner authorizes the qRD to remotely wipe the entire device in order to ensure that qRD data is securely removed from the device. Every attempt will be made to remove only qRD data, however there is no guarantee of this. The Device Owner will, under this scenario, forfeit the opportunity to review the data being removed.
- p. Device Owners agree that the qRD has the right to disconnect a personal Electronic Mobile Communication Device from qRD's corporate email system or disable services without notification or justification.

2.4 qRD Technical Service Department Responsibilities

- a. Technical Services Department staff will review all personal Electronic Mobile Communication Devices to confirm that they are not restricted for use in accordance with Section 2.2 of this agreement.
- b. Technical Services Department staff will assist Device Owners in connecting their personal Electronic Mobile Communication Device to qRD's corporate email system.

- c. Technical Services Department staff will conduct orientation training with Device Owners to ensure that the device will be used properly in service of the qRD.
- d. Personal Electronic Mobile Communication Devices will only be supported by the Technical Services Department on a “best effort” level.
- e. Technical Services Department staff will change a Device Owner’s qRD email account password to prevent additional email being delivered to the device and will immediately execute a remote wipe of the device if the Device Owner reports the device as lost, stolen or compromised.

2.5 Stipend

- a. The stipend rate for the use of a personal Electronic Mobile Communication Device will be calculated annually on January 1st at 75% of the cost of a reasonably equivalent Usage Plan purchased for a qRD-owned Electronic Mobile Communication Device.
- b. The stipend will be paid monthly to all Device Owners, except if the Device Owner is an Elected Official.
- c. The stipend is considered a taxable benefit.

As evidence of their agreement to be bound by the above terms, the qRD and the Device Owner each have executed this agreement on the respective dates written below:

qathet REGIONAL DISTRICT by
its authorized signatory

Al Radke, CAO

Date: _____

DEVICE OWNER:

[add Owner Name below signature

Date: _____