City of Pitt Meadows
THE Natural PLACE

ADMINISTRATIVE POLICY A002

04 - Information Systems & Services

Mobile Client Computing Technology

Effective Date: September 20, 2018
Last Revised: April 17, 2023
CAO Signature:

Policy Statement

1. The City of Pitt Meadows provides mobile client computing technology (herein referred to as 'City Mobile Devices') to elected officials, employees, volunteers and other persons (herein referred to as 'Users') for conducting City business. This technology may include cell phones, smartphones, tablets, laptop computers and mobile internet sticks. Issuance of these technologies is to be authorized by Department Directors under the terms of this policy. Anyone using City Mobile Devices must comply with all applicable federal and provincial laws, the specific conditions set out in this Policy and all other City policies as they apply.

Purpose

2. The purpose of this policy is to:

    a) Establish accountabilities and provide the terms under which Users with City Mobile Devices are expected to operate;

    b) Define requirements and responsibilities around the acquisition, use, standardization, management, and disposal of City Mobile Devices; and

    c) Establish a set of rules that limit the ways in which City Mobile Devices may be used at the City and set guidelines as to the proper use of this technology.

Scope

3. This policy applies to the use of City Mobile Devices that are owned, leased or licensed by the City of Pitt Meadows and applies regardless of their physical location.

Exclusions

4. The Chief Administrative Officer may grant standing or single instance exemptions to this policy where a valid business reason exists.

Policy

5. Definitions

(a) In this policy,

I. **Mobile Client Computing Technology**: Includes all cell phones, smartphones, laptop computers, tablet computers, mobile internet sticks, these devices' usage plans and their related peripherals.

II. **Usage Plans**: Any voice, text or data plan (or combination of) offered as a service by a wireless carrier (e.g. Bell, TELUS, or Rogers). Cell phones, smartphones and mobile internet sticks all require usage plans for full functionality. In addition, laptop and tablet computers that have built-in cellular data modems require usage plans in order to have cellular wireless connectivity.

III. **Cell Phone**: A mobile telephone with built-in access to a cellular network, offers voice and texting capability, and in some cases camera and personal digital assistant capabilities.

IV. **Smartphone**: A mobile phone offering voice, text, e-mail, calendar, internet browser, and the ability to run applications.

V. **Mobile Internet Stick**: A USB device with a built-in cellular data modem that provides internet access (via a wireless carrier and data plan) to any City Mobile Device that it is connected to.

VI. **Laptop Computer**: A compute device that is portable, offering built-in display, keyboard, and pointing device. Typically has Wi-Fi capability, and may also include cellular data connectivity (for internet connection through a wireless carrier).

VII. **Tablet Computer**: A compute device that accepts touch-based input directly to an LCD screen, rather than via mouse or keyboard (though optional keyboard/mouse options may exist provided they are detachable). Includes Wi-Fi capability, and may also include cellular data connectivity (for internet connection through a wireless carrier).

VIII. Primary Compute Device: A desktop, laptop, or tablet compute device that offers sufficient performance to run the City's standard operating system as well as most software applications used by the City. Suitable as a sole compute device for some City employees.

IX. City Client Technology Standard: A City document (DM # 140731) referenced within this policy that lists all City approved client hardware devices and accessories.

6. Roles and Responsibilities

a) Information Technology

I. Establishes and maintains corporate standards for City Mobile Devices and their usage plans

II. Supports City Mobile Device hardware and software

III. Budgets all renewal costs for City Mobile Devices

IV. Procures City Mobile Devices and their usage plans

V. Maintains an inventory of leased or City-owned mobile devices

VI. Conducts regular reviews of City Mobile Device use

VII. Arranges training for City Mobile Device Users

b) Department Directors or Their Delegates

I. Approves City Mobile Device requests in accordance with this policy

II. Ensures those who are issued a City Mobile Device are aware of and conform to this Policy

III. Budgets and manages all costs associated with the initial acquisition of City Mobile Devices

IV. Identifies personal use charges within their department that should be reimbursed to the City

V. Approves roaming plans or equivalent for Users travelling outside of the country who require the use of a City Mobile Device for work-related purposes

c) Senior Managers and/or Human Resources

I. Collects City Mobile Devices from Users at the end of their tenure and forwards those devices to Information Technology

II. Ensures Information Technology is made aware (with as much notice as possible) of City Mobile Device requirements for new Users.

III. Users with City issued Mobile Devices

IV. Reads, understands and adheres to the City Mobile Device Policy (this policy) and other City policies as they apply including A009 - Acceptable Use of Information Technology

V. Attends and participates in training sessions for City Mobile Devices when provided

VI. Protects City Mobile Devices from loss, damage or theft and/or immediately reports loss or damage of assigned City Mobile Devices to Information Technology

VII. Upon resignation, termination of employment, or at any time upon request, Users will be asked to produce the equipment and related peripherals for return for inspection and will also be required to produce their device PIN/PW and will ensure that any personal charge accounts associated with the device are deactivated (including for example Apple accounts). Users unable to present the equipment in good working condition within a reasonable time frame (i.e., 24 hours) will bear the cost of replacement. Users with outstanding debts for equipment loss or unauthorized charges will be considered to have left on unsatisfactory terms and may be subject to legal action for recovery of the loss.

7. Prohibitions

(a) n/a

8. Procedures and Guidelines

a) General

I. City Mobile Devices which have been damaged and will not be replaced should be reported to the Department Manager and to

Information Technology who will discontinue mobility plans and de-activate mobile capabilities for those devices.

II. City Mobile Devices which are not used for an extended period of time (more than one month) should be reported to the Department Manager and to Information Technology who will transfer the City Mobile Device to a minimum use plan.

III. If any User with a City Mobile Device is on leave (other than vacation), that device must be returned to Information Technology for temporary reallocation.

IV. Lost or stolen City Mobile Devices must be reported immediately to the Department Manager and to Information Technology. If stolen, individuals should report the incident to local police immediately.

V. The City may perform periodic audits of City Mobile Devices including the use of those devices.

b) Issuance of Mobile Client Technology

I. In general, the specific type(s) of City Mobile Devices issued may vary based on individual needs including application or software requirements, working environments and usage & mobility requirements.

II. The City Client Technology Standard (DM ref #140731) includes detailed issuance criteria and shall be used as a guideline to determine which device best meets an individual's needs. Conditions under which Users shall be considered eligible to receive City Mobile Devices will be maintained within the City Client Technology Standard.

c) Freedom of Information and Protection of Privacy

I. Activity records for City Mobile Devices, including but not limited to: individual calls, e-mails, text messages, pictures, videos, and internet access history is information that may be released to the public under the Freedom of Information and Protection of Privacy Act (FOIPPA).

d) General Acceptable Use

I. Users who are issued City Mobile Devices must use those devices in accordance with existing IT acceptable use criteria as outlined in Policy A009 – Acceptable Use of Information Technology (DM#1469).

e) Acceptable Personal Use

I. Personal use of City Mobile Devices must conform to all applicable conditions listed in Policy A009 Acceptable Use of Information Technology. The following additional conditions apply to the personal use of City Mobile Devices:

- Department Managers will review monthly invoices for their department and notify Users within their department where additional personal use charges are incurred. Users may be required to reimburse the City for overages or additional charges that result from personal use as directed by their Department Manager.

- It is the responsibility of Users to back-up any personal information (e.g. photos, videos, contacts) that is stored on City issued mobile devices. The City will not be held responsible for the loss of any such information

- It is the responsibility of Users to ensure any non-City standard media, software or content installed or used on City owned devices is done so in accordance with applicable terms, conditions and/or licensing agreements.

- Records resulting from the personal use of City issued mobile devices are information that may be released to the public under the Freedom of Information and Protection of Privacy Act (FOIPPA).

f) Use of City Mobile Devices While Operating Motor Vehicles

I. With the exception of fire personnel exempted under the Motor Vehicle Act Chapter 318, Part 3.1, Section 214, City Representatives are prohibited from using City Mobile Devices while operating a motor vehicle or motorized equipment. If a User is operating a vehicle, they should safely move out of traffic flow to the side of the road, put

the vehicle into park and turn off the engine, before using their mobile device

II. Users whose responsibilities include driving or equipment operation should refrain from using City Mobile Devices while driving a vehicle or while driving any other vehicle (borrowed or their own vehicle) while conducting City business. Drivers shall comply with all federal, provincial and local laws and regulations regarding the use of mobile devices including cell phones. Incoming or outgoing cellular phone calls are not allowed while driving. Sending or reading text messages, emails, dialing cellular phones, viewing television, videos, or DVD's and inputting data into laptop computers, personal digital assistants or navigation systems are prohibited while driving. The cellular phone voicemail feature should be on to store incoming calls while driving and all message retrievals and calls should be made after the vehicle is safely parked

III. Hands Free Exception – In situations where responsibilities include regular driving and acceptance of business calls, hands-free equipment may be provided by the City or individual. Special care should be taken in situations where there is traffic, inclement weather, or individuals are driving in unfamiliar areas. Under no circumstances are Users required to place themselves at risk to fulfill business needs. Additionally, all of the following conditions must be met:

- The device is not held in their hand;
- The device is secured in the vehicle in such a way that it does not obstruct the operators vision or impede the operation of the vehicle;
- The device is configured with a hands free accessory that is operated by voice recognition or activated by pressing a single button once to initiate or accept communication;
- If the hands free device is a headset or earpiece, the headset or ear piece must be in place prior to operation of the vehicle and may be attached to one ear only – not both.

g) Travel and Roaming

I. Using City Mobile Devices to send and receive texts, emails, place calls or use data (e.g. internet use or use of applications that use the

internet) while out of the country will incur additional costs to the City. Users are responsible for checking with IT to understand the rates that apply to voice and data use while outside of BC and Canada and to obtain their managers approval prior to using City Mobile Devices outside of BC and Canada. The following additional conditions apply to the use of City Mobile Devices outside of BC and Canada:

- The City will pay for a temporary roaming plan or equivalent if travel outside Canada is deemed necessary for work and the User must be in contact while away or the User is travelling outside of Canada for personal reasons but their responsibilities require them to maintain close contact with the City

- Users are responsible for requesting a roaming plan or equivalent from Information Technology prior to departure. Users may request a roaming plan or equivalent if travelling for non-work related purposes outside of Canada but will be responsible for reimbursing the City at the discretion of their Manager or Supervisor

- Approval of roaming plans or equivalent is the responsibility of Department Directors or their delegates

- Users are responsible for managing the use of their device while out of country to ensure that excess roaming fees are not incurred. If excess roaming fees are incurred and are not the result of the employee conducting City business then the User is responsible for reimbursement of those charges at the discretion of their Manager or Supervisor.

h) Cellular Data Consumption

I. While connected to any cellular network Users should avoid data-intensive activities when using City Mobile Devices particularly for personal use. City Mobile Devices contribute to a shared data pool from which all City Mobile Devices in turn draw from. Excessive use of data may result in the depletion of that pool leading to overage charges. The following are some examples of data-intensive activities which users should avoid when using City Mobile Devices for personal use and while connected to cellular networks:

- Streaming Video (For example a one hour hi-definition YouTube video can consume upwards of 3GB of data)

- Visiting websites that have embedded 'autoplay' video or audio (For example Facebook or Twitter)
- Video Chat
- Streaming Music
- Playing "On-line" Games

II. City issued iPhones will be provisioned with a 'Data Usage' app. This app is designed to track the consumption of cellular data against monthly billing cycles and alert Users who are nearing or exceeding monthly limits. Users are encouraged to use this app on a regular basis to monitor their data consumption.

i) Wi-Fi Data Consumption

I. Most City facilities have City managed corporate Wi-Fi which allows City devices to have connectivity to the internet without consuming data from the cellular network. Users should ensure City Mobile Devices are connected to the City's managed corporate Wi-Fi wherever possible as opposed to the cellular network.

II. Users may connect City Mobile Devices to their home Wi-Fi network and engage in data-intensive activities provided they do so under the conditions listed in this and other City policies as they apply.

j) Acceptable Wi-Fi Networks

I. Users may configure City Mobile Devices to connect with the following Wi-Fi networks:

- City Corporate Wi-Fi
- Home Wi-Fi (provided it is password protected)
- Government owned Wi-Fi (Federal, Provincial, Municipal)
- Wi-Fi owned and managed by reputable educational institutes
- Free public Wi-Fi that is provided through reputable ISPs including Shaw Go Wi-Fi and TELUS free Wi-Fi

II. Users may configure City Mobile Devices to connect with the following Wi-Fi networks provided this is kept to a minimum and only when no other acceptable Wi-Fi networks are available:

- Hotel Wi-Fi
- Conference Wi-Fi
- Airport Wi-Fi

III. Users may not configure City Mobile Devices to connect with the following Wi-Fi networks:

- Unknown Wi-Fi networks
- Privately owned networks including but not limited to coffee shops, restaurants and book shops
- Tethering to Wi-Fi mobile hotspots through non-City owned devices

k) Tethering

I. When using a City Mobile Device to create a Wi-Fi hotspot it is the Users responsibility to ensure that the device they are connecting is either a City owned device or a trusted personal device. Tethering is only permitted where no other acceptable options are available.

l) Location Tracking

I. The City will not use location tracking on any client City Mobile Device for the purpose of tracking Users or monitoring performance. The City may use mobile tracking capabilities only in the following instances:

- In the event of an Emergency Operations Center (EOC) activation where a City Mobile Device is issued to a User who has been assigned responsibilities in this situation
- The City Mobile Device is lost or stolen
- Tracking of a City Mobile Device is required by law to support a legal investigation

- The User to whom the City Mobile Device is issued has requested that location tracking be activated

- Purchasing and Installing Apps for Personal Use

II. Users may purchase and install apps on City-issued iPhone devices for personal use provided they do so in accordance with the conditions listed in this and other City policies as they apply. City IT may at any time require users to remove (uninstall) personal use apps from City issued iPhones if those apps have been deemed by IT to be a risk to the City. In such cases users must comply and remove the apps as directed by IT. Users may not purchase or install personal use (or business use) apps for any other type of City Issued Computing Device including laptop, tablet and desktop computers.

III. Personal use apps for City issued iPhone devices should be purchased and installed under the Users personal Apple ID.

IV. Personal use apps for City issued iPhone devices may only be purchased from the official Apple App store.

m) Purchasing and Installing Apps for City Business

I. IT will manage the purchasing and installation of apps required for business use on all City Mobile Devices. Requests to install new apps for business use should be submitted to IT support.

n) Jailbreaking iPhone and iPad Devices

I. Jailbreaking an iPhone or iPad device refers to the act of changing software on the device for the purpose of removing restrictions and limitations imposed by Apple.

II. Users should not jailbreak City issued iPhone or iPad devices under any circumstances.

o) Care and Protection of Mobile Devices

I. Mobile devices are easily lost, stolen and/or damaged. Users must exercise proper care of City issued mobile devices including:

- Not leaving devices unattended in a public place or in plain site within a vehicle, even if the vehicle is locked
- Ensuring devices are securely locked in a cabinet, drawer or office during non-working hours if the device is left at work
- Making reasonable efforts to avoid physical damage to the device including ensuring protective casing is on whenever possible
- Not using the device in inclement weather unless the device has been outfitted with a protective case

p) BYOD – (B)ring (Y)our (O)wn (D)evice

I. The City does not permit BYOD at this time.

q) Security and Device Management

I. IT will enforce basic security provisions on City Mobile Devices which may include but not be limited to device lock codes or passwords, time-durated auto locking of devices (where an individual must re-authenticate after a period of inactivity), account lock-out after a certain number of failed login attempts and drive encryption. Lock codes and/or passwords should not be shared by anyone.

II. Smartphones and tablets owned by Users will only be permitted to connect to the City's guest Wi-Fi network.

III. Any City Mobile Device may be remotely wiped if 1) the device is lost or stolen or suspected to have been stolen; 2) the User terminates his or her employment or tenure with the City; 3) IT detects a data or policy breach, a virus or similar threat that could impact the security of City staff, infrastructure or data.

r) Environmental Sustainability

I. Where possible, devices listed in the City's Client Technology Standard, including City Mobile Devices will adhere to industry environmental and sustainability standards.

II. City Mobile Devices will always be disposed of in environmentally responsible ways including reuse within economically challenged

areas or non-profit groups and recycled according to provincial e-waste standards and guidelines.

s) Cost and Lifecycle Replacement

I. Monthly usage costs, including overages of voice, text or data will be paid by the business unit to which the User is associated with.

II. There is no standard service duration for smartphone devices. These devices should be left in service for as long as they continue to meet business needs, are safe, functional and provide adequate performance and functionality.

III. The initial purchase cost of a City Mobile Device and accessories are to be budgeted by the department to which the User is associated with.

IV. Replacement of City Mobile Devices and accessories are to be budgeted within the IT department budget.

V. Managers within the business units or service groups will determine when business needs necessitate that a given device be replaced or upgraded.

t) Support

I. IT is responsible for providing support for City Mobile Devices including repairs, upgrades and replacement, set up, troubleshooting, un-packing and repacking.

II. iPhone Users are responsible for OS upgrades as and when prompted by the device.

u) Loaner Pool

I. In the event of a City Mobile Device failure IT will maintain a pool of spare devices at a rate of one loaner device for every 25 devices of that type.

v) Violations

I. Any violation of this policy may result in discipline (including suspension of user's privileges and/or system removal), dismissal, criminal charges and/or other legal action

Related Policies

9. Other related policies include:

   (a) A009 – Acceptable Use of City Information Technology

   (b) City Client Technology Standards