Mobile Device Guidelines for B.C. Public Service Employees

Mobile devices are portable and self-contained electronic devices that can connect to the government network. This includes but is not limited to laptops, tablets, smartphones, and cellphones. The use of mobile devices is essential in a fast-pace and dynamic work environment. While allowing employees to communicate and perform their duties remotely, mobile devices also pose a number of unique risks for privacy and security.

The purpose of this document is to provide employees with guidance on their use of mobile devices given current legal requirements, government policy, and best practices. It addresses the most commonly asked questions employees have about their mobile device use and management.

Many of the key requirements applicable to mobile devices come from the Appropriate Use Policy and the Information Security Policy. Employees must review the Appropriate Use Policy at the commencement of their employment, when they are issued a new device, and annually if they work with a significant amount of confidential information. Ministries may also have additional policies or guidelines related to mobile device use that employees are expected to follow.

Your New Mobile Device

I have just received a new mobile device. What is the first thing I need to do to set it up properly?

Government-issued smartphones and tablets must be enrolled in the Mobile Device Management Service (MDMS). This is required to access corporate email, calendar, and business applications. Along with your new device, you will also receive an email with detailed instructions on how to install the MDMS and complete the enrollment process. There are only limited circumstances for when a smartphone or tablet does not have to be enrolled in the MDMS, which are specified in the Mobile Device Security Standard.

Government-issued laptops and basic cellphones (which lack the technical capability to connect to wifi or use cellular data) do not require the MDMS. In addition, personal devices of any kind may not be enrolled in the MDMS at this time.

How can I choose a strong password and ensure it is protected?

The most important thing you can do to protect a mobile device is to have a strong password. Here are a few best practices to keep in mind:

- Your password should be difficult for someone else to guess, but easy for you to remember – a combination of numbers, symbols, upper and lower case characters increases the strength of your password;
- Never share your password with anyone (including an administrative assistant or technical support) and make sure to prevent others from viewing you enter it;
- Do not use your IDIR password for anything other than logging onto your government account (such as the password for a personal email account); and
- Remember that the strongest password is useless when it is written down and can be easily found (like on a sticky note next to your computer or taped to the device itself).

Using your Mobile Device

Can I use a government-issued mobile device for personal purposes?

Employees may use their mobile devices for a reasonable amount of personal use. Use must be limited during work hours and not interfere with your responsibilities, be legal, not compromise security, and never be used for financial gain. Use must also be consistent with the Standards of Conduct.

Can I store government information on a mobile device? What if I need to work from home?

Employees must store electronic records in protected government systems (for example, the network drives on a computer). The local hard drive on a mobile device is **not** considered a protected government system. When you are working outside of the workplace, this means you must save any files you need to your network drive and then access the network from home using a secure remote connection, such as Virtual Private Network (VPN) or Desktop Terminal Service (DTS). For more information, please see Section 3 of the Working Outside the Workplace Policy. You can also remotely access your email account on a laptop using the email web access site.

Only in extenuating circumstances may a record be temporarily stored on a mobile device. It must be absolutely necessary to do. In addition, you must follow the steps outlined in Section 11 of the Appropriate Use Policy. You must also remember that when conducting a search for records in response to a freedom of information request, any information stored on a mobile device is subject to that request.

These requirements do not apply to emails that are automatically stored, as duplicate records, on your mobile device by the government's secure email system.

I regularly work outside of the workplace, including in public places. How can I protect my mobile devices?

Because we often carry our mobile devices everywhere and use them in public spaces, the information on them is at greater risk of compromise. When working outside of the workplace, employees are expected to take appropriate precautions. Here are a few tips to protect your mobile devices and the information you are working with:

- Never leave your devices unattended in a public place;
- Prevent others from looking over your shoulder and trying to view what you are working on;
- Find a private place to take work-related phone calls;
- Store your mobile devices in a secure location when travelling (e.g. a hotel safe or the trunk of a car); and
- Avoid using public charging stations (i.e. where a charging dock or cable is already provided), such as on a ferry or in an airport, as these are not considered safe for use.

Can I connect my mobile device to a public wifi network?

You can connect to public wifi as long as it is from a known source (e.g. hotel or airport) and your device settings are configured properly to prevent unauthorized access to the government network and protect against external attacks. Never allow your device to connect automatically to an unknown network. If you require internet access to work on your laptop, however, it is recommended to instead create a "personal hotspot" with your smartphone and then connect your laptop to it. This will guard against any information you transmit from being intercepted by a third party (review the Self-Service Portal or contact 7-7000 for further assistance to learn more about setting up a personal hotspot).

Can I download new applications or software on my mobile device? Is there a process I need to follow?

You must have your supervisor's permission to download applications or software onto government-issued mobile devices. This is not meant to be a deterrent to prevent employees from downloading useful applications or software, but rather to promote awareness of both their benefits and potential risks.

- If an application or software is available through the iStore or Self-Serve Centre and also available from another source, you must download it from the iStore or Self-Serve Centre.
- If an application or software is **not** available through the iStore or Self-Serve Centre, there is a checklist supervisors can use to assess its privacy and security risks and determine if you need to seek further advice.
- You must never download any applications or software that:
    - Are prohibited by the Government Chief Information Officer;
    - Present unacceptable privacy or security concerns; or
    - Impose terms and conditions that are unacceptable to the government, such as indemnification clauses.
- There are legal restrictions against storing personal information on servers outside of Canada. This can be a problem if you trying to use Cloud-based applications (such as Google services or DropBox) or if an application is able to access the contacts and calendar you have saved on your mobile device.
- While you can use your mobile device for limited personal use, the restrictions set out above apply regardless if an application or software is intended for personal or business use.

As an employee, do I need to update the software or apply patches on my mobile device on a regular basis?

Employees must apply mobile device patches and update software, once they have been approved by Office of the Chief Information Officer, on a regular and timely basis commensurate with the confidentiality of the information on their mobile device and the level of risk. This helps correct flaws and improves the security of your devices.

Am I allowed to change the operating system or security settings on my mobile device?

You must never change or alter the operating system or security system settings on a government-issued mobile device. This is a process known as jailbreaking (on iOS) or rooting (on Android) – and is often attempted in an effort to install unauthorized applications. It is considered to be tampering and can significantly compromise the security of your device. Jailbroken or rooted devices cannot be connected to the government network until their status is corrected.

Traveling Abroad

I am travelling outside of Canada for work. Can I take my mobile devices with me?

Check first with your Ministry Information Security Officer as some ministries DO NOT allow employees to take government-issued mobile devices outside of Canada.

Given the increased risks involved, it is generally preferable to avoid the use of mobile devices whenever you are travelling abroad. If your ministry does permit it, there are a number of precautions you should take, both *before* and *during* your trip:

- Ensure tablets and smartphones are enrolled in the Mobile Device Management Service;
- Set-up your laptop in advance to access the government network using a secure remote connection, such as VPN or DTS. You may also securely access your email using the email web access site;
- Ensure government information is not stored on the local hard drives of any of your mobile devices; and
- Be vigilant in preventing your devices from being lost or accessed by others in public spaces.

Please see the Foreign Travel Tip Sheet for specific guidance and strategies to protect government information, and maintain security of this information, when travelling on government business outside of Canada.

There are additional restrictions against accessing personal information outside of Canada, which are discussed below.

Are there privacy concerns with accessing personal information while travelling?

Except in very limited situations, the *Freedom of Information and Protection of Privacy Act* prohibits personal information held by the government from being stored or accessed outside of Canada. More specifically, for employees, the legislation permits you to access personal information while travelling outside of Canada – such as on a laptop or smartphone – if it is *necessary* to perform your duties or if the information is immediately necessary to protect your health or safety.

Loss and Disposal

I have lost my mobile device! What should I do?

Mobile devices are small and portable, resulting in them being very easily lost or stolen. Given the potential for confidential information to be accessed by others, the loss of a mobile device is considered an "information incident." If you have lost a mobile device, you **must** report it immediately to your supervisor and follow the Information Incident Management Process. Remember that you need to report a mobile device *as soon as* it is judged to be lost and, for instance, not simply wait a couple days in the hopes it will turn up.

What is the proper way to dispose of old mobile devices?

For the procedures to follow when disposing of mobile devices, please visit the Asset Disposal Process website.

Further Information

I have a specific question or problem. Who can I contact?

For general questions about policy requirements and your responsibilities as an employee, please email IM.ITpolicy@gov.bc.ca. For questions specifically about privacy issues, please contact the Privacy Helpline at 250-356-1851 or privacy.helpline@gov.bc.ca.

For technical support and help with your mobile device, please call 250-387-7000 or email 77000@gov.bc.ca .