Board of Health Manual
Public Health Sudbury & Districts

Policy

Category
Board of Health Administration

Section
Technology

Subject
Board of Health Mobile Device Use

Number
I-V-10

Approved By
Board of Health

Original Date
February 2015

Revised Date
June 21, 2018

Review Date
September 15, 2022

Purpose
This policy applies to all Board members who use health unit-provided mobile devices to connect to Public Health Sudbury & Districts network as well as any form of wireless communication capable of transmitting packet data. Upon receipt of their mobile device, Board members will review and sign the attached form, *Board of Health Mobile Device Provided by the Public Health Sudbury & Districts.*

The health unit may, at its discretion and in accordance with this policy, provide mobile devices at the expense of Public Health Sudbury & Districts for Board of Health members for the purpose of fulfilling their duties as board members.

Mobile device includes any health unit owned or provided device that is portable and capable of storing, collecting, transmitting or processing electronic data or images including, but not limited to, laptops, tablets, cellular or smart phones and storage media.

Board Members are responsible for ensuring the appropriate use of the device as well as the security and safe keeping of the device as outlined in this policy and the supporting procedure.

Mobile devices are important tools for the organization and their use is supported to achieve business goals. Mobile devices can also represent significant risk to information security and data security and without security measures they can be a conduit for unauthorized access to organizational data.

The policy shall:

- Support board of health members to perform their duties using mobile devices
- Promote safety and security when using health unit mobile devices
- Limit organization risk and liability
- Reinforce current data and network security standards

Public Health Sudbury & Districts is required to protect its information assets in order to safeguard privacy, confidentiality, intellectual property and the organization's reputation.

The following rules apply:

- Devices must not be jailbroken* or have any software installed which is designed to gain access to functionality not intended to be available to the user. There should never be illegal or pirated software loaded on the device.
- While personal use of the device is permitted, personal use should not be contrary to organization policy or procedure and must not adversely impact device safety or security or the intended business uses of the device.
- Devices must never be used by other than the original user it was intended for.
- Board Members are prohibited from using the health unit-issued device while operating a motor vehicle.
- Board Members use of mobile devices must comply with Board of Health governance policies, practices and procedures including, but not limited to, conflict of interest, code of conduct and confidentiality.

All devices will be registered with Information Technology and will be managed by its Mobile Device Management software (MDM). MDM allows devices to have policies and applications applied to them as well enables Information Technology staff to remotely wipe the device in the event it is lost or stolen.

All devices prior to their return at the end of the term must have the Find My iPad turned off and the device password must be provided to the Executive Assistant to the MOH.

*To jailbreak a device is to remove limitations imposed by the manufacturer. This allows access to the operating system, thereby unlocking all of its features and enabling the installation of unauthorized software.