



Town of Wellesley

Bring Your Own Device Policy

Rev. 2.3

December 13, 2013

This document provides policies and standards for the Town's "Bring Your Own Device" (BYOD) program, which permits use of **personally owned smart phones and/or tablets** ("personal devices") by Town of Wellesley (Town) employees to access Town network resources. Access to and continued use of Town network services is granted with permission from their respective department head, and on condition that each user reads, understands, and follows this policy concerning the use of these devices and services.

1. Requirements for all BYODs Accessing Town Network Services

The Town's Information Technology Department (ITD) maintains a list of current personal devices approved for use in the BYOD program and establishes rules of behavior that may vary depending on the type of device or operating system configuration. Users:

- will not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or Town financial operations
- agree a complex network password is to be used to access email and network resources
- will maintain the original personal device operating system and keep it current with security patches and updates, as released by the manufacturer
- will not "jail break" the personal device (installing software that allows the user to bypass standard built-in security features and controls)
- agree to not share the personal device and network accounts with other individuals or family members, due to the business use of the device (access to Town e-mail and network resources)
- will delete any sensitive business files that may be inadvertently downloaded and stored on the personal device through the normal process of viewing e-mail attachments
- will not connect the personal device to the user's work PC via USB connections for file-sharing (document transfer) or backup purposes
- will immediately notify ITD if the personal device is lost or stolen, at which point ITD will change the user's complex network password

2. Expectation of Privacy

ITD personnel respect the privacy of your personal device and will only request access to the device to assist with implementation of security controls, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. While usage of the personal device itself is both personal and business, the Town's ITR Policy regarding the use/access of Town e-mail and other Town system/network services remains in effect.