

## Computer and Mobile Device Use

---

<b>Responsible officer:</b>	Director Corporate and Organisational Development
<b>Key Result Area:</b>	Organisational Improvement
<b>Document type:</b>	Policy
<b>Reference:</b>	10/01/0004
<b>Approved by:</b>	Council
<b>Date approved:</b>	24 February 2021
<b>Date of next review:</b>	February 2022

### Objective

The objective of this policy is to ensure that Council’s Information Technology assets, when deployed to Council employees, Councillors, contractors and volunteers for use in their Council duties, are appropriately cared for and are used for appropriate purposes only.

### Scope

Computers and mobile devices including laptops, tablets and smartphones are made available to staff and Councillors for use in their duties for Towong Shire Council. Mobile devices covered by this policy include both Council owned devices and approved non Council owned devices (BYOD).

### Information as a Council Asset

All information created or received including files and messages stored on users’ devices, the servers or electronic mail remain the property of Towong Shire Council. Misuse, illegal use, infringement of others use and unauthorised use are prohibited.

## Personal Use

Council devices are able to be used for personal use as long as the usage does not contribute to excessive additional wear and tear and does not infringe on the ability of others to use their devices. Council devices are not to be used for commercial purposes. Councillors are also governed by the Councillor Support and Expenses Policy in the appropriate use of Council devices.

## Misuse

Misuse of Council's Information Technology equipment is prohibited and includes:

- Using or distributing other user names and/or passwords;
- Copying programs or information illegally;
- Obtaining or using pirated software or illegal content;
- Intentionally or recklessly introducing computer viruses;
- Attempting to gain higher access to files or programs protected by security or password;
- Deliberately or recklessly damaging equipment or the information stored within it;
- Engaging in unsolicited bulk email;
- Using internet access in an unlawful manner;
- Using the internet to menace or harass others;
- Transmitting or viewing obscene, abusive or sexually explicit language or material;
- Distributing components designed to compromise system security;
- Using a mobile phone or other electronic device whilst driving or operating Council vehicles or Plant in contravention to the Road Safety Road Rules 2017 (Vic);
- Any other unauthorised use otherwise determined by Towong Shire Council.

## Mobile Device Usage

### *Council Owned Devices*

The IT Department will provide assistance with the creation of accounts and installation of software necessary to activate the device and connect it to the mobile network. The IT department will also acquire and install applications required for corporate use. Council will manage the devices under an Asset Management process and/or utilise a third party MDM software. Council has the right to block users from installing specific applications which have compatibility issues with council installed software, or which are deemed to be inappropriate in accordance with Council's expectations.

Council reserves the right to delete all corporate information from the device if requested and authorised by the user member's senior line management. Council has the right to audit the device, including applications and information, to ensure compliance with relevant Council policies.

Employee MUST contact the service desk as soon as possible if their phone or device is lost or stolen. The Service desk will then wipe all corporate data from the mobile phone or mobile device.

Devices MUST be configured with a secure device access password or passcode for use to access and lock the device when not in use.

Users must ensure personal consumption does not adversely impact Council operations or impose costs onto council, and ensure that council data is only sent through the corporate email system.

Upon termination of employment, the employee must return to their Supervisor their device which will be reset and all data deleted. Council will collect some information regarding the device, including version information, installed applications and location information.

#### *Non-Council Owned (BYO) Devices*

Devices must not be 'jailbroken' or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

The IT Department will acquire and install (or provide documentation to install) applications required for corporate use, and will pay for any license necessary to manage any device connected to the corporate network. Users are responsible for any costs associated with accessing Council Networks and Systems. Council takes no responsibility for any damage to devices caused by the installation of software necessary to manage and control corporate data on the device.

The IT Service desk will only provide support for issues relating to usage with council applications.

Council reserves the right to manage all devices that have access to corporate networks and systems. Council may collect some information regarding the device, including version information, installed applications and location information. Council reserves the right to delete all corporate information from the device if requested and authorised by the user member's senior line management.

Devices must be kept current by the users with the manufacturer's hardware and software patches or as instructed by the IT department.

Users MUST advise the IT Service Desk when the device is lost or stolen and the IT Department may wipe all corporate data from the device. Users are responsible for rapid replacement of their device should it be lost or stolen and should consider such mitigation strategies as arrangements with their vendor or replacement insurance.

Devices MUST be configured with a secure device access password or passcode for use to access and lock the device when not in use.

Users are responsible for the backup of all personal data on the device and for any application purchases which are used for personal use.

Upon termination of employment, all corporate Information and applications will be removed from personal device.

### **Deployment**

The Director Corporate and Organisational Development is responsible for overseeing implementation of this Policy.

### **Application of the policy**

This Policy is applicable to Towong Shire Council in all its operations and functions.

Council reserves the right to monitor, review and collect information regarding potential infringements and perform checks on user activity.

## Breaches

Breaches of this policy may result in disciplinary action up to and including dismissal. The police may also be contacted in instances where behavior is illegal.

## Resources

The following resources are committed by Council to assist with the implementation of this policy:

- The Director Corporate and Organisational Development is to oversee the implementation of this Policy;
- The Information Technology Officer is to implement this Policy; and
- Software and appropriate financial resources to extract data in order to assist with the implementation of this Policy.

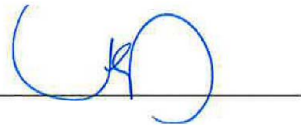
## Results

The deployment of this policy together with the results achieved will be reviewed at least annually.

## Human Rights Charter Compatibility

This policy has been assessed as being compatible with the *Charter of Human Rights and Responsibilities Act 2006 [Vic]*.

Authorised by: \_\_\_\_\_



Juliana Phelps  
Chief Executive Officer