# Elected Members Use of Council Hardware and Software Policy

| | |
|---|---|
| **Reference Number:** | 1.5 |
| **Type:** | Council Policy |
| **Category:** | Corporate Governance |
| **Relevant Community Plan Outcome:** | • Our values, leadership and collaborative approach are bold and courageous and enables us to deliver value for our community and create a leading liveable City<br>• The management of our city is progressive, responsive and sustainable to ensure a united and unique place for future generations<br>• Open and accountable governance |
| **Responsible Officer(s):** | Manager Information Services |
| **First Issued/Approved:** | July 1996 |
| **Minutes Reference:** | CoS 3/10/2023, Item 4.43 |
| **Last Reviewed:** | October 2023 |
| **Next Review Due:** | September 2025 |
| **Applicable Legislation:** | Copyright Act 1968 |
| **Related Policies:** | Electronic Communications Policy<br>Recruitment and Selection Policy<br>Mobile Device Policy |
| **Related Procedures:** | N/A |

## 1. Purpose

The City of Charles Sturt's technology system is integral to the ongoing and successful operation of the Council. The purpose of this Policy is to reduce the risk of electronic attacks, other threats, and vulnerabilities from impacting the computer network and systems environment of the Council.

## 2. Scope

This Policy applies to Elected Members using the City of Charles Sturt's computer equipment and network systems.

## 3. Policy Statement

All software applications and hardware computing equipment used to access The City of Charles Sturt's information and technology systems must be authorised by the Manager Information Services.

Specific authorisation must be received from the Manager Information Services prior to:

- installing or executing (running) a computer application or software program; or
- installing or connecting computer, network or other hardware devices to Council's computer system.
- installing or connecting to a cloud-based subscription software service (free or otherwise).

Once approval has been provided by the Manager Information Services, a record of the approval must be retained within the Council's records management system.

On computers with Windows 10 or above operating systems, the download and installation of applications via the Microsoft applications store is permitted. In the event that any application interferes with the functional operation of the device or impedes the ability of the device to perform required Council functions, the Manager of Information Service may elect to either have the application uninstalled or to return the device, in its entirety to the default settings in order to return the device to a functional state. In this event, Council is not responsible for the loss of personal data or settings.

The only pre-approved hardware which may be used are Universal Serial Bus (USB) data storage devices (e.g. 'flash drives') with inbuilt data protection mechanisms for the internal transport of data files between machines. No data storage device with executable programs (with the exception of data protection software), scripts or operating systems may be used at any time.

The introduction of unauthorised hardware, software or data which results in, or could result in, damage to Council's computer system may be dealt with by the Code of Conduct. Breach of any software licence by the installation of unauthorised software may also be dealt with under the Code of Conduct Policy.

**3.1 Personal Use of Software**

Council recognises that a restricted and discreet use of personal apps (not for business purposes) may occur, as with devices that have app based functionality, such as mobile phones.

- Use of personal apps must be lawful, must not incur material additional charges, must not interfere to otherwise fulfil your obligations to Council, and must not interfere with or adversely impact on Council's reputation.

- Such apps are only permitted to access sensitive Council information when installed via the Council's Mobile Application Management (MAM) platform.

- In the event that any personal app interferes with the functional operation of a Council device, or impedes the ability to perform required Council functions, the Manager of Information Services may elect to either have the app uninstalled or to return the device, to the default settings in order to return the device to a function state.

**3.2 Removable Media**

All Removable Media devices connected to Council technology systems are subject to the controls applied through endpoint protection, including but not limited to Anti-virus software.

Removable Media used to store Council sensitive information must be protected by in-built data protection mechanisms (e.g. encryption).

No Removable Media Device with executable programs, scripts, operating systems or malicious software may be connected to Council technology systems at any time.

## 4. Definitions

| Key Term – Acronym | Definition |
|---|---|
| Cloud based subscription software (free or otherwise) | Software in which data is maintained, managed and backed up remotely and made available to users over a network (typically the Internet) and can also be used for file transfer/sharing.<br>Non-approved Cloud Storage of Council information is not permitted. |
| Removable Media | Includes CD/DVD, USB devices or any other type of removable media used to store information. |
| Software | Software is a set of instructions, data or programs used to operate computers and execute specific tasks. Software is a generic term used to refer to applications, scripts and programs that run on a device. |
| Hardware | Hardware is the physical components that a computer system requires to function. |
| Dock | A docking station used to provide a simplified way to plug-in additional hardware devices to a laptop (e.g. external monitor, keyboard etc.) |