Mobile Device Policy (including BYOmD) – Council Members

Reference Number:	2.25
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
Responsible Officer(s):	Manager Information Services
First Issued/Approved:	March 2012
Minutes Reference:	CoS 3/10/2023, Item 4.44
Last Reviewed:	October 2023
Next Review Due:	September 2025
Applicable Legislation:	Local Government Act 1999 Broadcasting Services Amendment (Online Services) Act 1999 Electronic Transactions Act 2000 Equal Opportunity Act 1984 Copyright Act 1968 National Principles for the Fair Handling of Personal Information
Related Policies:	Council Member Behavioural Management Policy Use of Unauthorised Hardware and Software Policy Records Management Policy Electronic Communications Policy Council Member Allowance and Support Policy
Related Procedures:	E-mail Protocol BYOmD Connection Request Form

1. Purpose

The City of Charles Sturt recognises the need to embrace new and emerging technologies to improve the way business is conducted and contribute to improving the way the City meets its business objectives.

Mobile devices are a common and cost effective tool for information management and communication. In addition to the prevalence of mobile devices, Council Members are also increasingly requesting the option of connecting their own mobile devices (Bring Your Own Mobile Device – BYOmD) to Council equipment and networks.

The City of Charles Sturt views the use of mobile devices (both Council owned, and non-Council owned) as a positive IT practice that can be of significant benefit to users, IS and the organisation as a whole.

The City of Charles Sturt is responsible for maintaining effective security over all equipment and information within its environment.

Due to the portable nature of mobile devices there is a high requirement to maintain security for these devices and for any information stored or transmitted via them.

The purpose of this policy is to provide directives on the deployment, use and maintenance of mobile devices within the City of Charles Sturt so that:

- The correct processes and procedures are drafted and employed when utilising mobile computing devices and technologies, and;
- Council Members are aware of their individual responsibilities in relation to the use and security of mobile devices for the transmission and storage of information and access to the City of Charles Sturt systems and infrastructure.

2. Scope

This policy applies to all users of Council technology, equipment and services including:

- Council Members;

Council Members who use or access Council technology, equipment and/or services are bound by the conditions of this policy.

Mobile devices covered by this policy include both Council owned devices and approved non-Council owned devices of the following types:

- Notebook, tablet, laptop computer equipment;
- Smartphone devices used for mobile internet, data storage, calendars, contacts and task lists;
- Mobile phones where mobile internet (e.g. 3G/4G) technology is used for email correspondence;
- Smartphone devices capable of running third-party or downloadable applications (e.g. iPhone, iPad, Android, Windows Mobile, etc), and;
- All removable media including CD/DVD, USB devices or any other type of removable media.

3. Policy Statement

3.1 Use of Council Owned Mobile Devices

The following must be observed with respect to the use of Council owned mobile devices:

- All use of mobile devices, personally and professionally, must be appropriate and lawful;
- Only mobile devices owned and operated by City of Charles Sturt may be used to connect to the City of Charles Sturt infrastructure or services without prior approval from the Manager Information Services;
- Any installed management software, such as anti-virus software, must not be removed and must be kept up to date;
- Council owned mobile devices remain the property of the City of Charles Sturt and as such can be unreservedly requested and accessed by the Information Services Portfolio at any time;
- Any information which infringes copyright, or any other form of intellectual property rights, e.g.: music libraries, movies etc. is not to be stored on any device owned by the City of Charles Sturt;
- The user of the device must notify the Service Desk immediately upon loss, theft or suspected loss/theft of the device. Where possible, the contents of the device will be remotely erased and the services associated with the device will be disabled;
- USB memory sticks from an unknown or un-trusted source are not to be connected to the City of Charles Sturt equipment;
- City of Charles Sturt owned devices are locked to the City of Charles Sturt's chosen network provider. Transfer of such devices to other carriers will only be considered where a pressing business need is identified. In which case, service transfer costs may be investigated and any costs that can not be justified for business purposes may be passed on to the user of the device;
- Usage charges for mobile devices are subject to periodic review. Excess data usage may be investigated and any additional costs that cannot be justified for business purposes may be passed on to the user of the device;
- When using a council owned device that provides data enabled services, Council Members are required to monitor and manage data consumption levels using inbuilt data usage settings -;
- Council Members are responsible for ensuring mobile devices are not accessed by other persons that are not authorised to view information on the device.
- Council Members may not use any cloud-based apps or backup that allows Council-related data to be transferred to unsecure parties. Due to security issues, mobile devices should not be synchronised to other devices in the home.

- No modifications to device hardware or software or installing additional hardware or software unless approved by the Manager Information Services.

- Council Members are required to use Multi-Factor Authentication (MFA) when logging into their account. MFA provides enhanced security for user accounts. Traditional usernames and passwords can be stolen or guessed and are becoming more vulnerable. MFA is an effective way to protect Council's network from cyber-attacks if user credentials are compromised. MFA will appear as a push notification on mobile phones with the option to Approve/Deny the login.

3.2 Use of Non-Council Owned Mobile Devices

Council Members may be permitted to connect non-Council owned mobile devices to the City of Charles Sturt systems and infrastructure for the express purpose of receiving email, contact and calendar updates.

Permission to connect non-Council owned mobile devices to the City of Charles Sturt systems and infrastructure for the express purpose of receiving email, contact and calendar updates, can only be completed with express authorisation in writing by the Manager Information Services. This is due to licensing implications of connecting mobile devices to Council's network in particular Microsoft Exchange (email).

In addition to adherence to all other terms of this Policy, the use of a non-Council owned mobile device connected to the City of Charles Sturt network, requires acceptance and implementation of the following conditions and shall be confirmed by signature of agreeance to the conditions of this policy:

- The owner/user of the device recognises that their may be data cost implications from using the mobile device (particularly when accessing data from a 3G/4G network) and that these costs are required to be covered under the provisions of the Council Members Allowances and Support Policy.

- The owner/user of the device will accept the installation of a City of Charles Sturt-controlled profile, where it is deemed necessary, either at the initial time of connection or at any time thereafter, on the device. This profile will enforce certain configuration parameters including a timer lock with a mandatory passcode and a limit to the days of mail and calendar items stored on the device;

- The owner/user of the device must put in a PIN, password or passcode on every device that is used to access Council information;

- The owner/user of the device will notify the City of Charles Sturt Service Desk immediately upon loss, theft or suspected loss/theft of the device. Where possible, the contents of the device will be remotely erased, and the services associated with the device will be disabled;

- The user of the device agrees to protect Council information residing on the device, including ensuring that non-council agents and council agents that are not authorised and, do not have access to council information stored on the device;

- No City of Charles Sturt data other than mail (including attachments stored within the mail system), contacts and calendar items may be stored on non-Council owned devices unless expressly authorised in writing by the Manager Information Services;

- Non-Council owned devices will not be supported by City of Charles Sturt IS personnel with the exception of connectivity to City of Charles Sturt email services;

- City of Charles Sturt will accept no liability for functionality, serviceability or performance associated with the device and any responsibility with regard to warranty will reside solely between the owner/user of the device and the supplier/manufacturer;

- City of Charles Sturt accepts no responsibility or liability for the loss of Council related or personally related data residing on the device;

- City of Charles Sturt reserves the right to erase the contents of the device and/or disable the device at any time, and at its sole discretion.

- The installation of an MFA application is required to enhance the security of the City of Charles Sturt user account.

3.3 Physical Security of Mobile Devices

The following must be observed when handling mobile computing devices:

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible, they should be kept on the person or securely locked away, or special cable locking devices should be used to secure the equipment to a non-removable fixture;

- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended;

- Mobile devices should be carried as hand luggage when travelling by aircraft.

3.4 Protection of Information on Mobile Devices

The following must be observed in order to securely protect information on mobile computing devices:

- Every reasonable effort should be made to ensure that the City of Charles Sturt information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons;

- Mobile devices are not to be used as the sole repository for City of Charles Sturt information. All City of Charles Sturt information stored on mobile devices is to be backed up as appropriate.

3.5 Exemptions

This policy is mandatory unless an exemption is granted by the Manager Information Services. Any requests for exemptions from any of these directives should be referred to the IS Service Desk.

3.6 Breach of the Conditions of this Policy

In circumstances where a breach of this policy occurs, Council reserves the right to restrict the use or access to the technology or network, equipment, or services and to maintain that restriction at its discretion.

3.7 Indemnity by Non Employees

The Council bears no responsibility whatsoever for any legal action threatened or commenced due to conduct and activities of Council Members in accessing or using these resources or facilities. All Council Members indemnify the Council against any and all damages, costs and expenses suffered by the Council arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement.

Legal prosecution following a breach of these conditions may result independently from any action by Council.

4. Definitions

Key Term – Acronym	Definition
Anti-virus software	Protective software designed to defend computer equipment (including mobile devices) against malicious software.
Applications	A computer program that runs on computer equipment (including mobile devices) and performs a specific function.
App	A computer program that runs on mobile computer equipment that provides a specific function.
BYOmD	Bring Your Own Mobile Device. A trend in the IT industry of users (employees / agents) connecting their own mobile devices to organisational networks for access to organisational information.
Cloud-based	A term that refers to applications, services or resources made available to users on demand via the Internet from a cloud computing provider's servers.
Copyright	The exclusive legal right to reproduce, publish, sell or distribute the matter and form of something (such as a book, musical piece, artistic work or computer program).
Data enabled service	Access that enables a mobile device to send a receive data. This is usually via email, the internet or via mobile apps.
Intellectual property	The creations of the mind: ideas, inventions, literary and artistic works, symbols, names, images and designs used in commerce.
IS	Information Services Portfolio.
IT	Information Technology.
Laptop	A portable computer small enough to use on one’s lap.
Material	Includes data, information, text, graphics, animations, speech, videos and music or other sounds, accessible electronically, including any combination or selection of any of these.

Mobile and tablet devices	A small, often handheld computing device typically having a touch style screen and/or a miniature keyboard which is light weight.
Multi-Factor Authentication (MFA)	MFA provides enhanced security for user accounts. Each login from a network outside Charles Sturt (external network) to services protected by MFA (Such as Office 365, including Outlook) requires the user to authorise using the Microsoft Authenticator Application. This notification will appear as a popup push notification on the user's mobile phone with the option to Approve/Deny the login.
Notebook	A thin laptop.
Removable media	Includes CD/DVD, USB devices or any other type of removable media.
Security System	To protect the information on our network we have prescribed controls giving authorisation and access to files and directories in the network. Each individual has a series of passwords which allows them access to information and programs within their authority. Network security is controlled by Information Services staff and is overseen by General Manager Corporate Services.
Signature	A signoff clause which allows you to add your own name, title, Council contact details, email address, direct telephone number, etc. at the end of outgoing emails.
Smartphone	A mobile phone with internet access.
USB memory stick	A small device used for storing files. Usually about the size of a thumb. Connects to other computer devices via the USB port.
3G/4G	Wireless connectivity platform for mobile devices.