Bring Your Own Device Policy

Document Name	Document Version Number	Review Date
Bring Your Own Device Policy	1.0.5	June 2024
Date Adopted	**Minute Number**	**Status**
18 June 2020	5608	Revised

Purpose

Greater Hume Council recognises the need to embrace new and emerging technologies to improve the way business is conducted and contribute to improving the way the Council meets its business objectives.

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

Scope

Councillors, staff, contractors and volunteers who use or access Councils network, technology, equipment and/or services are bound by the conditions of this policy.

Mobile devices covered by this policy include any device or accompanying media that you may use to access the systems and data of Greater Hume Council, whether they are Council owned devices and approved non-Council owned devices.

Definitions

BYOD – Bring Your Own Device. Any electronic device owned, leased or operated by an employee or contractor of Greater Hume which is capable of storing data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers and netbooks.
IT – Information Technology.
User – a person who has authority to use an application, equipment, or system owned by Greater Hume Council.

Policy Content

The Greater Hume Council 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 Greater Hume Council so that:

- The correct processes and procedures are drafted and employed when utilising mobile computing devices and technologies, and;
- Users 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 Greater Hume Council's systems and infrastructure.

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 Greater Hume Council may be used to connect to Greater Hume Council infrastructure or services without prior approval from the Information Technology Coordinator;
- 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 Greater Hume Council and as such can be unreservedly requested and accessed by the Information Technology Coordinator at anytime;
- 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 Greater Hume Council;
- The user of the device must notify the Customer Service Officer - Holbrook 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 Greater Hume Council equipment;
- Greater Hume Council owned devices are locked to Greater Hume Council'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 cannot 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, users are required to monitor and manage data consumption levels using the management software provided;
- Users are responsible for ensuring mobile devices are not accessed by other persons that are not authorised to view information on the device.

Use of Non-Council Owned Mobile Devices

Councillors, staff, contractors and volunteers may be permitted to connect non-Council owned mobile devices to Greater Hume Council's systems and infrastructure for the express purpose of receiving email, contact and calendar updates.

Permission to connect non-Council owned mobile devices to Greater Hume Council's 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 Director Corporate and Community 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 Greater Hume Council's 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 will notify the Information Technology Coordinator 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 Greater Hume Council 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 Information Technology Coordinator;
- Non-Council owned devices will not be supported by Greater Hume Council IT personnel with the exception of connectivity to Greater Hume Council services and Salary Sacrifice computer equipment when utilised for work purposes;
- Greater Hume Council 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;
- Greater Hume Council accepts no responsibility or liability for the loss of Council related or personally related data residing on the device;
- Greater Hume Council reserves the right to erase the contents of the device and/or disable the device at any time, and at its sole discretion.

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.

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 Greater Hume Council 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 Greater Hume Council information.
- Users are responsible for backing up and restoring the data and configuration settings of your BYOD. Personal data is not to be backed up to or stored by Greater Hume. Council is not responsible for any personal loss or damage suffered by actions undertaken by Greater Hume to protect Council's data stored on your BYOD.
- All Council information stored on mobile devices is to be backed up as appropriate and uploaded into Council's EDRMS (InfoXpert) as soon as possible.

Exemptions

This policy is mandatory unless an exemption is granted by the Director Corporate and Community Services. Any requests for exemptions from any of these directives should be referred to the Information Technology Coordinator.

Breach of the Conditions of this Policy

In circumstances where a breaches 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.

Indemnity by Non Employees
The Council bears no responsibility whatsoever for any legal action threatened or commenced due to conduct and activities of Users in accessing or using these resources or facilities. All Users 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.

Any employee identified of using a Council supplied mobile phone in a manner that is unacceptable/inappropriate will be subject to disciplinary action and possible criminal prosecution.

Variations to Policy
The General Manager or his delegated representative be authorised to approve variations to this policy, provided such variation does not result in additional cost being incurred by Council.

Links to Policy
Records Management Policy
Internet, Email and Computer Use Policy
Model Code of Conduct Policy
Performance and Misconduct Policy
Volunteer Policy
Information Technology Security Access Policy

Links to Procedure
Records Management Procedures
Information Technology Security Access Procedure

Links to Forms
Personnel Security Access Form – Mobile Phone/Device
Personnel Security Access Form – VPN Remote Access
Personnel Security Access Sub Form - Network

References
Nil.

Responsibility
Director Corporate & Community Services
Information Technology Coordinator

Document Author
Manager Corporate Services

Relevant Legislation
Local Government Act 1993
Broadcasting Services Amendment (Online Services) Act 1999
Electronic Transactions Act 2000
Privacy Act 1988

Associated Records
Nil.