Bring Your Own Device (BYOD) and Mobile Device Policy

Document Name	Document Version Number	Review Date
Bring Your Own Device (BYOD) and Mobile Device Policy	1.0.6	May 2027
Date Adopted	**Minute Number**	**Status**
21 May 2025	6865	Revised

Purpose
Greater Hume Council recognises the need to use various technologies to meet its business objectives.

The purpose of this policy is to outline how mobile devices will be utilised within the organisation.

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

Scope
This policy applies to everyone using a Council Mobile or approved BYOD when accessing Council's information and ICT resources, including employees, volunteers, labour hire, contractors, Councillors or professional services consultants.

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

For the purpose of this policy, mobile devices comprise any equipment that connects to a network using a SIM Card or similar device and accessing the Council's information and ICT resources except laptops. This includes but is not limited to satellite phones, mobile phones, tablets, modems, photographic and recording equipment.

Definitions

BYOD Mobile Device	The practice of allowing employees of an organisation to use their own smartphones, or other mobile devices for work purposes. BYOD 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, they include but are not limited to satellite phones, mobile phones, tablets, modems, photographic and recording equipment (excluding laptops).
Council Mobile Device	A mobile device which Council has provided to an employee to assist them in their daily work activities as required by their role. The Council device is considered an asset of Council to be used accordingly.
Employee	Any individual employed, appointed, or otherwise attached to Council, whether on an ongoing, temporary, contractor, casual or voluntary basis. This includes all senior executives and secondees from other agencies and may include contractors and employees of any firm or company contracted to perform work on behalf of Council subject to the nature of the policy and its application.
Mobile Device	For the purpose of this policy, mobile devices comprise any equipment that connects to a network using a SIM card or similar device and accessing Council's information and ICT resources. This includes but is not limited to satellite phones, mobile phones, tablets, telemetry devices, modems, photographic and recording equipment. Laptop computers are specifically excluded under the scope of this policy.
Mobile Device Management (MDM)	Mobile Device Management is the process of securing, monitoring and supporting the use of mobile devices, such as smartphones and tablets, in the workplace. The function of MDM is to control data, configuration settings and applications on all mobile devices used within a company or organisation.
Mobile Threat Management (MTM)	A secure mobile gateway for a Council owned device allowing Council to secure the mobile device against any threats.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: A) Whether the information or opinion is true or not; and B) Whether the information or opinion is recorded in a material form or not *(The Privacy Act 1988).*
User	A person who has the authority to use an application, equipment, or system owned by Greater Hume Council.

IT	Information Technology – a broad term that involves the use of technology to communicate, transfer data and process information.
ICT	Information and Communication Technology- encompasses the infrastructure, tools and systems that enable modern computing and communication including devices like computers, the internet and telecommunication.

Policy Content
Council is responsible for maintaining the security of ICT and information stored within its environment. Due to the portable nature of mobile devices there is a requirement to maintain security for these devices and for any information stored or transmitted via them.

This Policy outlines the following requirements associated with the use and application of mobile devices by Council and ensures the correct processes and procedures are adhered to when utilising mobile computing devices and technologies:

- Employees 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.
- The risks introduced by using mobile devices are minimised and managed.
- The correct processes and procedures are developed and employed when using mobile devices and technologies.
- Mobile devices used for the Councils' purposes are protected by appropriate security measures consistent with the security requirements.

All use of mobile devices, personally and professionally, must be appropriate and lawful.

Eligibility
An employee may be eligible to have a Council-owned Mobile Device if it is deemed necessary to their position, and at their manager's discretion. The type of mobile devices offered by Council are at the discretion of the IT Coordinator and vary depending on the Employee's role. This is so Council can ensure the devices are supported via our technology program and that the employee has a device appropriate to their role. The range of mobile devices available will be restricted to reduce support costs. Alternatively, an employee may choose to use their own personal mobile device to access and connect to Council systems and programs.

In order to connect to Council infrastructure or services, users will be required to ensure acceptance of terms and conditions as detailed in the policy.

A Mobile Device Management (MDM) solution must be installed on all Council Mobile Devices, to enforce minimum security settings necessary to protect Council systems and information stored or available on the mobile device. A MDM solution must be enabled on BYOD Mobile Devices where users wish to access Council systems and data from their device.

Access to Council information and applications will only be available through approved software (e.g. Outlook for email, Teams for messaging and collaboration) on managed mobile devices.

Council reserves the right to remove the MDM application from the device at any time without prior notification.

The MDM application on BYOD Mobile Devices may be removed by the owner of the device. Once the MDM application has been removed, Council applications and data can no longer be accessed from the device.

On Council Mobile Devices, removal of the MDM application must only be done by an authorised IT Coordinator or representative. As a part of this process, all Council data stored on the device will be removed and access to Council systems will no longer be available.

Use of Council-owned Mobile Devices

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

- Council owned mobile devices remain the property of Greater Hume Council and as such can be unreservedly requested by and accessed by the IT Coordinator at anytime.
- The User of the device must notify the IT 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.
- Greater Hume Council owned devices are configured 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.
- Council-owned devices will also be enrolled in a Mobile Threat Management (MTM) program which will protect the device against cyber security attacks.
- 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.
- Users are responsible for ensuring mobile devices are not accessed by other people that are not authorised to view information on the device.
- Council-owned devices will be allocated a PIN. If the PIN is modified the IT Coordinator must be notified via email or text message. Upon exiting the organisation, Council-owned mobiles must be returned to People & Culture, if the council-owned device cannot be accessed (due to an unknown PIN) Council reserves the right to withhold the cost of the mobile device from the exiting employee's termination pay.
- If an employee is unable to return the Council-owned device then Council may charge the Employee to reimburse Council for the cost of the mobile device.
- If an Employee seeks to retain the Council issued SIM and associated costs upon existing of the organisation, then the Employee will be required to place their request in writing for the General Manager to consider.
- Chargers, wall sockets and protective cases are to be provided and returned upon exit of the organisation or where a mobile device is being replaced.
- Employees are required to sign a Personnel Security Access Form – Mobile Phone/Device that details the mobile device and accessories that have been issued.
- Employees are required to ensure their Council-owned device is charged and in good working order to enable them to remain contactable during work hours.
- Employees are required to set up an appropriate voice mail message that identifies their name and Greater Hume Council. Employees should regularly check their voice mail messages and return calls within a suitable time frame.
- When issued with a Council-owned mobile, the Employee has a responsibility to respond to work related communication within a reasonable timeframe.
- Certain positions will have Council issued mobiles and these numbers will be provided to external parties such as Rangers that are on-call to the public.

- For employees that have a Council issued mobile, there is a requirement to share work mobile numbers with fellow internal staff and relevant stakeholders.
- Employees have a Right to Disconnect and therefore (unless on-call) may choose not to respond to work calls outside of work hours.
- Employees may use their Council-owned device for personal use. On these mobile devices, any other applications may be installed at the user's discretion, but personal applications must not have access to Council services and should minimise data usage.
- If an employee requires an application that has not been previously approved, then the Employee is to seek approval from the IT Coordinator.
- The Employee is obligated to report illicit or inappropriate content on their device or that of another Employee to their Manager.
- All employees that have a Council-owned mobile device and use the mobile while operating a vehicle are required to install hands-free (or Bluetooth) in work vehicles. Mobile phone usage while operating vehicles is required to be lawful. If an employee receives a fine for non-lawful use of a mobile device, Council do not accept any liability for such acts and employees are personally liable for any fines.
- Calls that attract a higher rate such as 1300 numbers are restricted. Calls that are competition lines, for gambling or questionable in view of Council's acceptable use policy are prohibited.
- Council recognises from time-to-time accidents may occur where a mobile device is broken. Greater Hume Council will replace the phone with a 'like' phone. Careless or reckless use of Council issued mobiles will not be covered.
- Any information which infringes copyright or any other form of intellectual property rights (e.g. other music libraries, movies etc.) must not be stored on any device owned by Council.
- Mobile and data access when travelling overseas is very costly. With manager approval, the IT Coordinator will arrange for the activation and subsequent deactivation of international roaming for Council mobile plans as well as data packs on an "as needs" basis. International voice call and data service usage (e.g. internet, email, streaming etc.) must only be used when essential. While overseas, personal use must be minimised otherwise the employee may be liable for excessive mobile usage fees. Council is not responsible for any costs incurred using BYOD Mobile Devices.

Use of non-council owned Mobile Devices (BYOD)

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, calls and use of relevant applications by way of the MDM and as outlined in Eligibility Section of this Policy.

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 is financially responsible for their data usage and costs associated with the phone.
- The owner/user of any device must accept an MDM solution to enforce minimum security settings necessary to protect Council systems and information stored or available on the mobile device.
- The owner/user of the device will notify the IT Coordinator immediately upon loss, theft or suspected loss/theft of the device. Where possible, the work apps and content of the device will be remotely removed 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 agents not authorised 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 IT Coordinator.

- Non-Council owned devices will not be supported by Greater Hume Council's IT department for trouble shooting issues with the exception of connectivity to Greater Hume Council services.
- 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.
- Council is not liable for replacement of damaged, broke, lost or stolen phones.
- 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 remove or restrict work related applications at the discretion of the organisation.
- Council or its agents will not be able to, nor will they access any personal applications, data or content.
- Council or its agents will not supply the Owner's mobile number to any external party, however if the Owner is agreeable, the mobile number may be shared internally for the purpose of receiving calls.
- Excess data usage on a personal phone is the employees responsibility and Council is not liable for excess data charges.
- A user can remove MDM from their non-owned Council device. If this occurs the IT Coordinator will be notified, and the employee will no longer be able to access Council ICT.
- For BYOD Mobile Devices, Council applications and data must be managed separately from personal application data.

Dual Sim Mobile Device

Employees who are eligible for a Council-owned mobile device may elect to have a Dual Sim Mobile Device so that they are not required to have two mobile devices. If the Employee elects to they can select either:

  - A Council-owned device with Council Sim and personal Sim
  - A non-owned Council device with Council Sim and personal Sim

- Users have the option to nominate business or personal mobile data. Users can nominate business data for work hours and switch to personal data for out of business hours phone usage.
- All Users of a Dual Sim must read and adhere to the items detailed under Use of Council-owned Mobile Devices.
- Users have the option to nominate business or personal phone contacts. Users can call contacts with the choice of selecting if they call from their business or personal number.
- Users have the right to disconnect from business calls and Council Sim when on personal leave by disconnecting the Council Sim for the leave period or after business hours.
- When an employee using this option leaves Council then the Council-owned device must be returned to People & Culture. Users are responsible for removing all personal data before handing device back in on final day of work.
- If an employee elected a non-owned Council device, the IT Coordinator will remotely remove all business-related data on final day of employment.

Misplaced, stolen, damaged or breached mobile devices

Council expects all employees to take reasonable care of Council Mobile Devices. It is the employee's responsibility to take all necessary measures to ensure a device is not damaged, lost or stolen.

The user of the mobile device must notify the IT Coordinator and their manager immediately upon loss, theft, breach or suspected loss, theft, breach of a managed device. In these circumstances, Council services associated with the device must be disabled. For BYOD Mobile Devices, only Council applications and data will be removed.

Costs for lost or damaged Council Mobile Devices will be billed to the employee's cost centre.

If the Council Mobile Device is faulty or damaged, an assessment will be made as to whether the device can be replaced under warranty.

Protective cases are provided with all Council Mobile Devices and must be used to shield the devices from undue wear, tear and damage.

Use of Mobile Devices around Children

The National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code) addresses child safe practices for the use of electronic devices while providing early childhood education and care (ECEC). Educators within our ECEC services working under the National Quality Framework (NQF) are obliged to adopt the National Model Code as a further support to promote a child safe culture.

Taking images or videos of children while providing Early Childhood Education and Care

Greater Hume Council acknowledges that a part of caring for and providing early education care requires the use of Council-owned mobile devices to conduct general activities such as taking photos, recording information, communication with parents and guardians, etc. The following conditions need to be adhered to in any of our Early Childhood Educate and Care environment's:

- Only Council-owned mobile devices should be used when taking images or videos of children while providing education and care and should be in accordance with The National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code).
- Personal electronic devices that can take images or videos (such as tablets, phones, digital cameras, smart watches) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage) should not be in the possession of any person while providing education and care and working directly with children. Any exceptions to this should be for limited, essential purposes that are authorised in writing (or through another means if written authorisation is not reasonably practicable) by the approved provider at the service, and where that access does not impede the active supervision of children.
- Essential purposes for which use and / or possession of a personal electronic device may be authorised for purposes other than taking images or recording videos of children include:
    - communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises
    - personal health requirements, e.g. heart or blood sugar level monitoring
    - disability, e.g. where a personal electronic device is an essential means of communication for an educator or other staff member
    - family necessity, e.g. a worker with an ill or dying family member
    - technology failure, e.g. when a temporary outage of service-issued electronic devices has occurred
    - local emergency event occurring, to receive emergency notifications through government warning systems, for example, bushfire evacuation text notification.

Use of Mobile Devices during work hours

Use of Mobile Phone devices during work hours for non-work activities. Employees and Users of mobile devices need to abide by the following:

- Restrict personal use of mobile phones during work hours unless on a break.
- To minimise distractions of other employee's move away to take calls of a personal nature.
- Minimise volume on mobile devices when indoors.
- When in meetings and in formal settings, ensure mobile devices are placed on silent.
- When on Lifeguard duties at Swimming Pools Lifeguards should not be distracted from focusing on the users of the pool. Personal Mobile devices should only be used for emergency calls or to receive calls from Council staff. All other mobile phone use is prohibited.

Purchase of Equipment and Ownership

Council is the legal owner of all physical and electronic information, computing and communication technology resources created or acquired to conduct Council's business. For BYOD, ownership applies to only the related Council information and specifically excludes the device itself.

Council delegates to its employees, daily management responsibility and custodianship of information and ICT resources for their use, maintenance and protection. With best effort and due care, employees are responsible for upholding Council's policies to protect Council's information and ICT resources.

Council-owned Mobile Devices must be purchased through approved channels. Individuals or business units must not buy their own Council Mobile Device. To obtain a Council-owned mobile device the Employee's Manager will need to obtain and complete the Mobile Phone Service Request Form.

Upon exiting the organisation all Council-owned mobile devices and accessories must be returned to People & Culture (or delegated Council representative) in good working order.

Usage and Service Charges

To protect public interests in the use of public resources, employees have no inherent right to use Council's ICT resources for non-council purposes. To this end, Council Mobile Devices should be primarily used for authorised business purposes; however, limited personal use is permitted if it does not have an adverse impact on Council use and services.

Exemptions

This Policy is mandatory unless an exemption is granted by the Director Corporate and Community Services or the General Manager. Any requests for exemptions from any of these directives should be referred to the IT Coordinator.

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.

Access to and storage of any material that could be considered offensive, obscene, pornographic, threatening, abusive, discriminatory, bullying or harassment, or may otherwise be considered illegal or unethical, is prohibited from any Council device. Such use may result in disciplinary processes in accordance with the Code of Conduct. Legal prosecution following a breach of these conditions may result independently from any action by Council.

Failure to Comply with this Policy
Ethical and behavioral standards that employees are expected to demonstrate while working with Council are set out in the respective Code of Conduct. If employees fail to meet those standards, corrective action may be taken in accordance with the respective Code of Conduct.

Individuals who are not Council sector employees such as volunteers, contingent or labour hire workers, professional services contractors and consultants may have their services, contract or agreement terminated immediately, or legal action could be taken if they are found to have violated this policy.

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.

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

Acceptance conditions:
Employees/Users are required to accept and adhere to the outlined terms and conditions and shall confirm by signature of the Personnel Security Access Form – Mobile Phone/Device to confirm their agreeance to the conditions of this Policy.

Where the above terms are not accepted, access to Council systems and data (e.g. Outlook email and Teams) will not be available from the mobile device.

Links to Policy
Records Management Policy
Internet, Email and Computer Use Policy
Model Code of Conduct Policy for Local Councils in NSW
Performance and Misconduct Policy (currently under review)
Volunteer Policy
Information Technology Security Access Policy
Child Safe Policy
Children Services - Child Protection 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
Personnel Security Access Form - Mobile Phone/Device
Mobile Phone Service Request Form

References
Nil.

Responsibility
Director Corporate & Community

Document Author
Director Corporate & Community Services

Relevant Legislation
NSW Local Government Act 1993
Broadcasting Services Act 1992
NSW Electronic Transactions Act 2000
Privacy Act 1988
ACECQA - National Model Code for Early Childhood Education & Care

Associated Records
Nil.