Accessing Council information via “BYOD” (Bring your own device)

<table>
<thead>
<tr>
<th>Department</th>
<th>Strategy &amp; Business Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Officer</td>
<td>Manager</td>
</tr>
</tbody>
</table>

Introduction

Mobile devices, such as smartphones, netbooks, laptops, and tablet computers, are important tools for the organisation and their use is supported to achieve business goals.

However, mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation’s data and Information & Communication Technology (ICT) infrastructure. This can subsequently lead to data leakage and system infection.

Bega Valley Shire Council has a requirement to protect its information assets in order to safeguard its customers, its intellectual property and its reputation. This document outlines a set of practices and requirements for the safe use of mobile device(s).

The purpose of this procedure is to identify accepted protocols for accessing Council’s information from non-Council issued equipment. The procedure facilitates the protection of customer information and that Council meets its legal requirements in this regard.

All Councillors, staff and contractors engaged by Council must adhere to this procedure which encompasses:

- All device(s), whether owned by Bega Valley Shire Council or owned by employees, that have access to corporate networks, data, information and systems, not including Council’s ICT managed device(s). This includes smartphones, netbooks, laptops and tablet computers but is not limited to these devices alone.

- Exemptions
  Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk and security assessment will be conducted by authorised ICT staff.

Council is obliged to comply with all current Australian legal provisions governing copyright protection for computer software supplied to Council.

Council must comply with the Australian Privacy Act 1988 Act no. 119 of 1988 as amended. Councillors, staff and contractors are also subject to the act and must therefore ensure information contained or stored on any device(s) complies with the act and to ensure such information is neither lost nor exploited.

Councillors, staff and consultants must comply with all licensing or purchasing terms and conditions required by suppliers that regulate the use of any software Council purchases or leases.

Using your own personal device/s

Council will not accept or agree to meet any costs associated with a personal employee’s device(s) or the usage of the device(s). Council would recommend that the private user investigate and evaluate options for insuring their personal device(s).
Council further recommends that the user constantly monitors their usage of the technology to protect themselves from un-planned costs associated with any usage of the device(s).

Using device(s) that are partially funded by Council

Depending on the position held by an employee, Council may agree to contribute a fixed amount toward the running costs associated with the device(s). This is at the discretion and approval of the Group Manager or Executive Manager of the section. If Council contributes toward these costs, Council may at its discretion, disclose the number of the device(s) internally and externally to allow for the device(s) to be used to contact the individual for the purposes of conducting Council business.

Technical requirements

1. Device(s) must be kept up to date with manufacturer or network provided patches.
2. Device(s) must be configured with a secure password. This password must not be the same as any other credentials used within the organisation.
3. With the exception of those device(s) managed by ICT, devices are not allowed to be connected directly to the internal corporate network.
4. Council will utilise MDM (see definitions) software to protect its information. Whilst the premise of this software is to segregate Council information from user’s information, Council cannot guarantee that user information will not be stored on Council archive systems. All costs associated with MDM will be met by Council. By using an MDM, the data will remain separate from the employee’s private data and charges.
5. Council’s use of MDM software allows Council to purge Council information from any device(s). This functionality includes the removal of any installed “apps” on the device(s) associated with any Council accounts.

User requirements

Specific processes that must be adhered to by Councillors, staff members (irrespective of whether an employee or contractor) and consultants are:

1. Users must only load Council information essential to their role onto their device(s).
2. Users must report all lost or stolen devices to Council’s ICT department immediately.
3. Users must report all device replacements to Council’s ICT department immediately. Failure to do this may see Council ICT department deem the unregistered device as an unauthorised access, that would see security breach action initiated, which could include, but is not limited to, the remote wiping of the device(s).
4. If a user suspects that unauthorised access to company data has taken place via a device they must report the incident to Council’s ICT department immediately.
5. 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.
6. Users must not load pirated software or illegal content onto their device(s).
7. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact ICT Helpdesk.
8. Devices must be kept up to date with manufacturer or network provided patches. As a minimum, users should be check for patches weekly and apply at least once a month.
9. Users must be cautious about the merging of personal and work email accounts on their device(s). They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Council’s ICT Helpdesk immediately.
10. Users must not use corporate workstations to backup or synchronize device(s) content.
11. It is the user’s responsibility to backup personal information and “apps” and Council is no way responsible for the loss of any information on the device.
12. ICT department only provides support services to Council provided hardware device(s) and software.
13. Council will under no circumstances sanction the making or use of unauthorised software copies by Councillors, staff or consultants. Council will take disciplinary action, if any staff member or consultant is found to be engaging in the unauthorised duplication of software. Depending on the circumstances, this action may include termination.
14. Councillors, staff members and consultants are required to notify their manager or the ICT Manager of any illegal copying of software or related documentation of which they become aware.
15. Council Information contained on or in devices is considered and remains the property of the Council.

Permitted use

Subject to the basic premise and purpose the following applies:

1. Councillors and staff must sign an agreement before accessing Council information with non-Council issued devices. This agreement may be incorporated into existing system access agreements.

Sanctions

Users who violate any of the conditions of this policy may be subject to disciplinary action including (but not limited to) written warnings and revocation of access privileges. Council also retains the right to report any illegal violations to the appropriate authorities.

Other relevant documents

This procedure is to be read in conjunction with policy 5.09 Information Technology as well as policy 5.02 Behaviour of Councillors and Staff.

It is also to be read in conjunction with procedures 5.09.1 Internet, Intranet and email acceptable use, 5.09.2 Mobile phone usage, and 5.09.5 Information Security.

Definitions

Mobile Device Management (MDM) is a type of security software used to monitor, manage and secure employee’s mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organisation. Mobile device management software is often combined with additional security services and tools to create a complete mobile device and security management solution. The MDM would be in the form of an application that would be installed on the device/s.
Attachment: BYOD usage agreement

I, (print name) ______________________________ acknowledge that I am being granted permission to access Council information from non-Council issued device/s and agree that my use will be conducted in accordance with Council’s policy governing the use thereof.

I understand that the basic premise of this policy is that it is intended to protect Council information and not to entrap people making reasonable efforts to safeguard Council information.

I understand that Council information contained on or in equipment is considered and remains the property of the Council at all times.

I understand that Council may at any time, use it discretion, to erase all Council information from the hardware.

I acknowledge that access to Council’s information is a privilege and can be withdrawn at any time.

I understand that I have been given notice in accordance with section 10(2) of the Workplace Surveillance Act 2005 (NSW); and that Council will be entitled to, and shall commence monitoring, all my personal and business use of these services and communication facilities, and that monitoring will be in accordance with this policy and that inappropriate usage may be cause for disciplinary action up to (but not limited to) written warnings and revocation of access privileges.

I understand that I must comply with the Australian Privacy Act 1988 Act no. 119 of 1988 as amended and will ensure information contained or stored on any device complies with the act.

I understand that if I am not prepared to accept any of the conditions of this policy that access to Council information will NOT be granted and permission to access the BYOD facility will be refused.

I understand that by signing this document that I acknowledge that I have read and understood this document. I further understand that it is my responsibility to seek advice regarding any questions that I might have regarding this document prior to my signing.

Signed ______________________________ Date __________________________

Witness name ______________________________ Witness signature ______________________________