AUSTRALIAN DENTAL ASSOCIATION VICTORIAN BRANCH

ADMINISTRATIVE BRANCH POLICY STATEMENT 03.09

BYOD

1. INTRODUCTION

1.1 This document defines the expectations that ADAVB has for the use of personally owned devices such as smart phones, tablets, and/or computers by ADAVB and other authorised personnel to access ADAVB resources and/or services.

1.2 Authorised personnel are permitted, subject to approval, to bring their own personal digital devices (BYOD) for use for ADAVB business purposes.

1.3 Where possible, devices owned by ADAVB members, staff and other authorised personnel (e.g. staff employed by Professionals Australia) may be used in place of ADAVB-issued technology, e.g. meeting room laptops.

1.4 Access to and continued use of ADAVB electronic resources is granted on the condition that each user reads and follows the ADAVB's policies concerning the use of these resources and/or services. This policy is intended to protect the security and integrity of ADAVB's data and technology infrastructure.

1.5 In allowing authorised users to BYOD for business purposes, the Branch acknowledges that some level of increased risk must be accepted, given that not all aspects of the BYOD security can be controlled by the Branch.

1.6 Non-adherence to this policy may expose the Branch to considerable risks, including security breaches, data loss, reputational damage and legal liability.

1.7 Personnel who BYOD are therefore expected to exercise a reasonable level of caution and responsibility when using their personal device to access ADAVB data, including agreement to and adherence to this policy.

1.8 Any queries regarding the safe use of a personal device may be directed to the CEO.

2. LEGISLATION

2.1 Relevant legislation includes:

- Health Records Act 2001 (Vic)
- Healthcare Identifiers Act 2010 (Cth)
- My Health Records Act 2012 (Cth)
- Privacy Act 1988 (Cth)
- Spam Act 2003 (Cth)

3. GLOSSARY

3.1 Document Sharing

ADAVB uses Cloud Services to securely share documents with Branch Council and committee members and other approved recipients.

3.2 Cloud Services

Cloud services are IT resources that include servers, storage and software delivered over the internet.

3.3 ADAVB Wi-FI

ADAVB maintains a secure wireless intranet to enable the conduct of its business. Access to the network is granted to authorised persons for the specific conduct of such business.

3.4 Jailbroken

iOS jailbreaking is the process of removing software restrictions imposed by iOS, Apple Inc's operating system, on its devices including the iPhone, iPod touch, iPad, and second-generation Apple TV. Jailbreaking permits applications, extensions, and themes unavailable through the official Apple App Store to be downloaded.
Unauthorized modifications to iOS ('jailbreaking') bypass security features and can cause numerous issues to the hacked iPhone, iPad, or iPod touch, including security vulnerabilities, instability, inability to install iOS updates and inoperability.

3.5 Rooted

Gaining access to the lowest level (root level) of the Android operating system is prohibited on stock devices. Rooting gives the user administrator rights to alter the OS, tweak the hardware and unlock the phone from its carrier. Rooting is required for more advanced and potentially dangerous operations including modifying or deleting system files, removing pre-installed applications, and low-level access to the hardware itself (rebooting, controlling status lights, or recalibrating touch inputs.) Security risks are inherent in this process.

4. ACCEPTED DEVICE TYPES

4.1 The following device types are acceptable for registration on ADAVB's Bring Your Own Device mobility service:

Accepted Device Types	Standard issue devices, such as tablets, smartphones, laptops, and personal computers are acceptable
Accepted Operating System Versions	Standard operating systems are acceptable, e.g. iOS, Windows, Android etc.
Unaccepted Devices and Operating System Versions	**Jailbroken or rooted devices are not acceptable for use on ADAVB's Wi-Fi, for accessing the ADAVB Cloud Services, or accessing any other ADAVB information or services.**

5. APPLICATIONS TO BE USED FOR ACCESSING ADAVB DATA

5.1 Applications that are acceptable for use on devices that access ADAVB data are those that are available through iTunes, the Mac App Store, or Google Play

5.2 Custom applications that are not available through these avenues are not acceptable for use on devices that access ADAVB data, as they may pose a security risk. Limited exceptions to this rule may apply, subject to approval by management.

6. MOBILE DEVICE MANAGEMENT (MDM)

6.1 As part of the ADAVB's information security framework, the organisation reserves the right to deploy and administer Mobile Device Management (MDM) software on any personally owned device that is used to access, store, or transmit ADAVB data or to connect to ADAVB networks, systems, or applications.

6.2 The MDM system will enable the ADAVB to implement and enforce appropriate security controls, including but not limited to device encryption, password complexity requirements, screen lock configurations, and the installation of security certificates.

6.3 ADAVB may, at its discretion, remotely manage, restrict, or revoke access to resources where a device is identified as lost, stolen, compromised, or otherwise non-compliant with established security standards. The ADAVB also reserves the right to execute a remote wipe of corporate data when necessary to protect confidential information.

6.4 The ADAVB affirms that the deployment of MDM software will be limited to legitimate business and security purposes. The MDM solution will not be used to access or monitor personal data, including but not limited to personal applications, photographs, messages, contacts, or browsing history. However, employees acknowledge that in the event of a full device wipe or other security action, incidental loss of personal data may occur. Employees are therefore responsible for maintaining independent backups of personal information.

6.5 When personnel leave ADAVB employment or cease serving in any official capacity such as committee membership , ADAVB reserves the right to execute a remote wipe of any organisational access and data on the BYOD device.

7. APPROVAL PROCESS

Prior to granting access to ADAVB Cloud Services users must read and understand this policy

8. CONFIDENTIALITY

Users are expected to keep confidential all files accessed through the ADAVB Cloud Services .

8. REIMBURSEMENT

8.1 Branch Councillors are eligible for an annual information and communications technology (ICT) allowance (which includes BYOD costs), in accordance with 1.02 BPS Finance.

8.2 Committees are not eligible for reimbursement or ICT allowances for BYOD used for Branch business

8.3 ADAVB employees are not generally eligible for allowances or reimbursement for BYOD, however this is subject to the discretion of management, usually confirmed upon the employee's commencement.

9. SECURITY

9.1 All personnel authorised to use ADAVB IT facilities are asked to familiarise themselves with basic IT security issues and protective measures. Guidance offered by the Australian Signals Directorate is recommended.
In order to prevent unauthorised access, devices must be password protected using the features of the device. Passwords for WiFi and ADAVB Cloud Services access will be set by ADAVB following the protocols for Windows and Microsoft passwords.

9.2 Passwords provide the first line of defence against unauthorised access to a personal digital device. The stronger the password, the more protected a device will be from hackers and malicious software. Personnel are required to ensure strong passwords are created for all accounts on the device.
A strong password should be at least eight characters long, include an alpha-numeric combination in upper and lower case and at least one symbol. Only the authorised user should know this password, the password should not be a word, date or name, and should not be used for any other device or application password. This password should be changed regularly.
The device must lock itself with a password or PIN if left idle for five minutes.

9.3 Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network as they are a security threat.

9.4 Smartphones, tablets and laptops belonging to employees that are for personal use only are not permitted to connect to the network.

9.5 Access to ADAVB data is limited based on user profiles defined by management and automatically enforced.

9.6 Users have responsibility to ensure no other person has access to ADAVB data they access or store on their BYOD.

9.7 A different password should also be used to access the folder in which ADAVB files are temporarily stored.

10. LOST/STOLEN DEVICES

10.1 If a personal digital device is lost or stolen, the owner is responsible for reporting the event as soon as practicable to the CEO, who will contact the ADAVB Business Operations Manager

10.2 In the event of a lost or stolen device the ADAVB or its authorised IT partner may exercise its right to execute a remote wipe of all organisational data through the use of MDM tools and applications.

11. DEVICE DATA PRIVACY AND CONTROL

11.1 USE OF ADAVB WI-FI

- BYOD devices may connect only to the Guest and BYOD WiFi networks. BYOD devices may not connect to the ADAVB Staff network as this allows direct access to the contents of the file server.

- ADAVB may remotely monitor information transmitted over ADAVB Wi-Fi to and from any network device to ensure adherence to Branch Policies and observation of legal requirements.

- ADAVB will not access or monitor personal digital device/s in any other way. This differs from the policy for ADAVB-provided equipment and/or services, where employees do not have the right to privacy while using equipment and/or services.

11.2 ACCESSING ADAVB Cloud Services

- Authorised personnel may use their personal digital devices to access their ADAVB Cloud Services and files for which they are members or authorised guests.
- Personnel may not access the ADAVB file server using any BYOD device.
- The ADAVB Cloud Services administrator will provide each user with an account. Upon receiving the account, users can access ADAVB Cloud Services using different access points.
- The password issued by the Branch should be amended as soon as practicable by the user and recorded securely and privately.
- The ADAVB Cloud Services can be accessed using any modern web browser
- The ADAVB Cloud Services must only be used for ADAVB business purposes.

11.3 ANNOTATION, SECURITY AND DISPOSAL OF MEETING PAPERS AND OTHER FILES ACCESSED THROUGH ADAVB CLOUD SERVICES

Access to and use of meeting papers

- Meeting papers are generally PDF documents, which may be viewed and annotated in Adobe Acrobat or on a tablet app such as Good Reader or iAnnotate.
- Where required, some Committees may be permitted to download copies of meeting documents for off-line reference and annotation. However, given the sensitivity and confidentiality of Defence, Disputes and Ethics, and Honours and Award Committee papers, these are not available for download and will require internet access for secure online viewing only.
- All personnel are asked to delete annotated copies of meeting papers within three months after the corresponding meeting, so that the only discoverable documents are the master copies held by the Branch.

All files

- ADAVB files should not be shared with others unless they are publicly available files.
- All files developed by the ADAVB or ADA Inc and stored on ADAVB Cloud Services remain the property of ADAVB.

Protection of ADAVB data on a personal digital device

- Authorised personnel are expected to take reasonable measures to protect the integrity and security of Branch data. For example, care should be taken when opening, viewing and storing sensitive or confidential information.
- Any Branch data personnel are authorised to have access to may be viewed on a personal digital device.
- Branch information, documents, and confidential data that are subject to legal or professional privilege must not be stored on personal digital devices and/or unapproved cloud-based services.
- Branch data must only be backed up to approved locations either within Branch systems or approved cloud service locations or providers.
- Where possible, ensure that automated cloud backup only applies to personal data, not ADAVB data.
- Take reasonable steps to reduce the risk of losing personal data. For example, store personal data separately from ADAVB data through file partitions or using a separate memory card.
- Owners are responsible for backing up and restoring the data and configuration settings of a personal digital device. Personal data must not be backed up to or stored by ADAVB.
- The Branch is not responsible for any personal loss or damage owners may suffer by actions undertaken by ADAVB to protect Branch data stored on a BYOD.

12. IT SUPPORT

12.1 Connectivity issues are supported by ADAVB's IT consultant, however the device manufacturer or their carrier should be contacted for operating system or hardware-related issues.

12.2 In the case of ADAVB staff, devices may need to be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

12.3 Councillors, Committee members and others, will be responsible for downloading and installing the applications needed to access the ADAVB cloud storage environments.

13. ACCEPTABLE USES OF ADAVB IT RESOURCES

13.1 ADAVB defines acceptable business use as activities that directly or indirectly support the business of ADAVB. ADAVB defines acceptable personal use on work time as reasonable and limited personal communication or recreation, such as reading or checking personal emails.

13.2 Employees may use their mobile device to access the following ADAVB owned resources:

- Email
- Calendars
- Contacts
- ADAVB files, which they are authorised to have access to
- Membership database

14. UNACCEPTABLE USES OF ADAVB IT RESOURCES

14.1 ADAVB has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted. See 15 below regarding the consequences of a breach of this requirement.

14.2 Devices accessing ADAVB Wi-Fi may not be used at any time to:

- Store or transmit illicit materials
- Harass others
- Take photos, videos or recordings of confidential ADAVB material, images, information on white boards, presentations, or voice recordings.

15. CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

15.1 The Branch will view non-compliance with this policy as a serious risk to data security and will therefore take any necessary steps to protect its data.

15.2 For ADAVB Members who are authorised to access the ADAVB Wi-Fi or Cloud Services, non-compliance with this policy may result in disciplinary action, such as the loss of access privileges and removal from a committee

15.3 For others who are not ADAVB personnel, but who are authorised to access the ADAVB Wi-Fi or Cloud Services, non-compliance with this policy will result in the loss of access privileges.

15.4 For ADAVB employees, non-compliance with this policy may result in disciplinary action, in accordance with 1.19 BPS Employee disciplinary.

15.5 In the event that deliberate non-compliance with this policy results in the Branch incurring legal action, reputational damage or data loss, the Branch will take necessary steps to recover data and financial losses and repair reputational damage.

16 UPDATING

This advisory document shall be updated every Council term.

Branch Policy Statement Number	03.09
Adopted by Council	27 November 2020
Reviewed by Constitution & Policy Committee	06 November 2025
Amended by Council	8 December 2024
Related Policies	BPS 1.02 Privacy BPS 2.01 Finance BPS 3.08 Use of Member Contact Details