Bring Your Own Device

1. Purpose

To outline the conditions of use for Department of Health (department) staff using personal devices for work purposes in accordance with the Bring Your Own Device (BYOD) Policy.

2. Applicability

This procedure is applicable to Department of Health employees using personal devices for work purposes whether permanent, fixed-term, contract or casual.

3. Procedure requirements

The following requirements apply to use of BYOD:

- **Awareness**: Staff must remain vigilant to their surroundings. Be aware of what is visible to others and lock the screen when not in use.
- **Security:** Confidential data or information must must be kept secure at all times. Where personal devices are used for the capture or transport of WA health system data or information, such data or information must be transferred to WA health system storage as soon as practicable.
- **Records management**: Any WA health system data or information processed via a personal device must be saved to an official records management or clinical/business system as soon as possible.
- **Software:** When downloading any software (personal or business) to a personal device, staff must exercise a high degree of caution. Software must always be sourced from reputable providers/or official app stores. Staff must make themselves aware of the privacy policy and licencing requirements of all software they install.
- **Travel**: If travelling overseas officially or privately, staff must remove any WA health system data, information or stored account details from their personal device unless authorised to retain by their manager. WA health systems and services may have geoblocks in place, and will not function if accessed from outside of Australia
- **Ceasing use**: Staff must ensure they delete any WA health system data, information and software before exiting the department, ceasing use of BYOD or leaving the device with a third party for repair.
- **Department Wi-Fi:** Staff are to ensure they have manager approval to connect personal devices to the department Wi-Fi for work purposes. Department Wi-Fi is not to be used on personal devices for personal use.

Staff should be aware that:

- usage of WA health system corporate network services may be monitored, logged and retained
- any damages or criminal/civil charges resulting from unlawful use of the personal device are the responsibility of the staff member (e.g. breaches of the Road Traffic Code)
- the department does not provide ICT support for personal devices, is not responsible or liable for the maintenance, backup, or loss of any data or information on a personal device, and does not accept responsibility for the loss, theft, or damage of a personal device.

Department staff are not obligated to use their personal devices for work purposes, and anyone doing so accepts the associated risks, including:

- in the event health authorities or law enforcement need to access or search for WA health system data or information on the device, personal devices may be seized by police
- any additional costs incurred through use of BYOD (e.g. through increased internet usage, software requirements) are the responsibility of the user
- personal health and safety (e.g. increased fatigue or stress from always being connected to the workplace).

3.1 Approved BYOD services

The only WA health system corporate network services that staff are permitted to access from personal devices are detailed in the table below.

APPROVED SERVICES	ACCESSED VIA	NOTES/GUIDANCE
Microsoft 365 Provides access to services including (not inclusive): • Microsoft 365 (Outlook, Word, Excel, PowerPoint, OneNote) • OneDrive • Teams, SharePoint • Power BI, Planner, MS Forms	http://www.office.com https://ww2.health.wa.gov.au/Global-Items/Staff-portal	Requires use of multi-factor authentication at each logon. Refer to the WA Health *M365 Acceptable Use Guidelines*.
Azure virtual desktop (AVD) Provides access to: • Mapped network drives • WA Health intranet (HealthPoint) • Microsoft 365 including Microsoft Teams • Electronic documents and records management system (EDRMS) • Corporate administrative and clinical applications.	Access guidelines available via the Staff Portal: https://wahealthdept.sharepoint.com/sites/hss-customer-ict-support/SitePages/ict-user-guides.aspx	All staff internet access via AVD is monitored to the same level as in the workplace. Data or information is not to be transferred from within AVD to any personal or cloud data storage service.

APPROVED SERVICES	ACCESSED VIA	NOTES/GUIDANCE
WA Health public websites Provides access to public information, WA health policies, and some specific portals intended for staff-only use.	https://ww2.health.wa.gov.au/	
MyFX and MyFT Provides secure messaging and document access services.	https://myfx.health.wa.gov.au https://myft.health.wa.gov.au	Ensure that any data or information accessed from this service is stored securely and not retained on the BYOD.
Approved cloud services	Links provided by system/data custodians on a per-case basis	Cloud-based services may be approved for specific staff to use.

3.2 Security

In addition to the required security controls included in the BYOD Policy the following additional controls are recommended:

- **Encryption:** Full hard-disk (or whole-of-device) level encryption should be enabled.
- **Location tracking software:** Location tracking capabilities activated where available to help find lost or stolen devices.
- **Home Wi-Fi:** Where a home Wi-Fi network is used by a BYOD to access department or WA Health systems, at a minimum there should be a router in place that supports WPA2 encryption. This should also be protected by a lengthy administration passphrase, comprised of at least 12 characters.

4. Related documents

The following documents are mandatory pursuant to this procedure:

- Bring Your Own Device Policy

5. Supporting information

The following documents inform this procedure (i.e. documents are not mandatory to the implementation of this procedure but may *support* implementation):

- Connecting to Wifi at Royal Street

6. Approval and review

This mandatory procedure is approved in accordance with the approval authority described in the Policy governance procedure and will be reviewed as required to determine effectiveness, relevance and currency. At a minimum it will be reviewed within 2 years after first issue and at least every 3 years thereafter.

Version	Effective from	Effective to	Amendment(s)	Authorisation
1.0	XX Month 2022	XX Month 2024	Original version	Deputy Director General

The review table indicates previous versions of the mandatory document and any significant changes.

The owner of this procedure is the **Director Corporate Services, Office of the Deputy Director General**.

Enquiries relating to this procedure may be directed to DoH.ICT@health.wa.gov.au

This document can be made available in alternative formats on request for a person with a disability.