Bring Your Own Device (BYOD)

1. Purpose

To set out requirements for secure and controlled use of personal devices for work purposes within the Department of Health (department) to ensure WA health system data, information and systems are protected in accordance with *MP 0067/17 Information Security Policy* and in support of the objectives of the *WA Health Digital Strategy 2020-2030*.

2. Applicability

This policy is applicable to Department of Health employees whether permanent, fixed-term, contract or casual.

3. Policy requirements

The following principles apply to the use of personal devices for work purposes.

- Staff make informed decisions about the use of their personal devices for work purposes, including any impacts on their health, safety and privacy.
- Flexible and remote working arrangements are supported.
- Risks to the security, confidentiality, integrity and availability of WA health systems, data and information are managed to acceptable levels.
- WA health system data and information is protected and handled appropriately in accordance with the relevant legislation.

3.1. Permissible use of BYOD

Staff may:

- use a personal device to access only the approved BYOD services detailed in the BYOD procedure
- connect personal peripheral devices (such as a mouse, keyboard, or fan) to a workplace machine for purposes such as charging as long as they do not transmit data or information and do not require additional drivers or software.

3.2. Non-permissible use of BYOD

Staff may not:

- physically or wirelessly connect any personal device to the WA health system corporate network at the workplace for the purposes of local network or internet connectivity
- connect a dedicated personal mass storage device (e.g. USB thumb drive or removable hard drive) to the WA health system corporate network or department-owned devices
- use a personal device to store or transfer any WA health system data or information via personal cloud-based storage or private email services (e.g. Drop Box, Gmail, Google Drive, Apple Cloud).

3.3. Roles and responsibilities

Staff who choose to use any personal device for work purposes must:

- appropriately maintain, secure and use their personal device, and manage the information contained on it, in accordance with applicable law, the Information Security Policy, and the BYOD Procedure
- acknowledge that utilising personal devices whilst at the workplace for any purpose inconsistent with this policy may constitute misconduct and be subject to disciplinary action
- immediately report any theft or loss of the personal device to their manager and the HSS Service Desk to determine the appropriate course of action
- understand and manage the potential impacts associated with this use. The staff member accepts all liability for their personal data and information and is solely responsible for minimising any potential data or information losses or any additional costs incurred.

Managers must ensure:

- this BYOD Policy and Procedure is communicated effectively to employees, including at commencement and termination of employment
- possible breaches of security, unauthorised access, misconduct or other human resources matters in relation to BYOD are investigated in accordance with relevant policies or procedures (e.g. Discipline policy, Information Breach Policy).

Health Support Services will:

- undertake security reviews of proposed new BYOD-accessible services
- oversee capture of access and usage logs.

3.4. Security

The following controls must be implemented for BYOD:

- Access control: All personal devices must have at least one access control method enabled (e.g. PIN, password, fingerprint, or facial recognition). Access codes must be kept secret and be unique to the staff member and the device (e.g. not used for common access by family members or used across all devices).
- Physical security: Personal devices must be configured to lock or logout if left unattended for more than five minutes.
- Antivirus/malware protection: Up-to-date antivirus/malware protection must be installed.
- Operating system: All recommended operating system updates from the manufacturer must be installed on the device once available. Compromised devices, including 'jailbroken' or 'rooted' devices which cannot be upgraded to the latest operating system are not permitted for BYOD use and may be disconnected from the WA health system corporate network without notice.
- Mobile Wi-Fi: Approved services may not be accessed via public or open Wi Fi access points, including ones with passwords. Mobile hotspots (via the staff members' private or work-provided phone) must be used instead.

4. Compliance monitoring

Usage of approved applications through BYOD may be monitored, logged and retained for review and audit.

5. Related documents

The following documents are mandatory pursuant to this policy:

- BYOD Procedure.

6. Supporting information

The following documents inform this policy (i.e. documents not mandatory to the implementation of this policy but may be best-practice and support implementation):

- *State Records Act 2000 (WA)*
- *Freedom of Information (FOI) Act 1982 (WA)*
- *MP 0067/17 Information Security Policy*
- *MP 0135/20 Information Breach Policy*
- *MP 0145/20 Information Storage Policy*
- *MP 0146/20 Information Classification Policy*
- *WA Digital Health Strategy 2020-30*
- *Microsoft 365 Acceptable Use Guidelines*.

7. Definitions

The following definitions are relevant to this policy.

Term	Definition
BYOD	Bring Your Own Device (BYOD) refers to the practice of using a personally-owned device for work purposes.
Corporate device	A device owned by the employer and issued to staff members for work purposes, for example, a corporate laptop, tablet or smartphone and peripheral devices.
Data	Unprocessed information.
Information	Data that has been processed in such a way as to be meaningful to the person who receives it.
Jailbroken or rooted device	Where software restrictions put in place by manufacturers to enhance data and information security have been removed from the device.
Peripheral device	Any device a user might connect to a workstation/laptop including keyboards, mice, hard drives, fans/chargers, etc.
Personal device	A personally-owned device used to access, store, or process work-related data or information. Personal devices include: • mobile devices (e.g. laptops, tablets, mobile phones, smart devices) • personal computers (e.g. home office desktop computers) • peripheral devices.
Personal information	As per the *Freedom of Information Act 1992,* means information or an opinion, whether true or not, about an individual, whether living or dead – • whose identity is apparent or can reasonably be ascertained from the information or opinion; or • who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.

8. Approval and review

This mandatory policy is approved in accordance with 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 policy and any significant changes.

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

Enquiries relating to this policy 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.