Corporate Mobile Devices

1. Purpose

To set out requirements for the control and use of mobile devices owned by the Department of Health (department) and provision of department funded mobile devices and data services in accordance with MP 0066/17 Acceptable Use of Information and Communications Technology Policy and MP 0067/17 Information Security Policy.

2. Applicability

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

3. Policy requirements

Employees who are provided with mobile devices and/or mobile and data services for work purposes must:

- assume responsibility for the physical security of the device, along with the information contained within
- adhere to local traffic laws and the driver distraction section of the Safe Driving Guidelines for WA Government Agencies regarding use of mobile devices in vehicles
- immediately report a lost or suspected stolen device as soon as it is discovered to be missing
- acknowledge that any personal data or information stored on the device may be wiped or remotely deleted if the device is lost or stolen
- ensure access control is enabled that is unique and not shared with other people
- ensure that the device is locked and kept secure when not in use
- ensure that the latest operating system updates are installed when they become available
- return a damaged department owned device for repair
- return a department owned device when no longer required to be used for department purposes
- monitor usage and minimise the service cost where possible.

Employees must not:

- use the device or service for inappropriate or improper use
- use the device when the operating system is no longer supported by the vendor and the hardware cannot be updated
- use the device to transfer any work-related information via personal cloud-based storage or private email services (e.g. Dropbox, Gmail, Google Drive, Apple Cloud)
- jailbreak or root the device, nor install an operating system or software that is not supported by the vendor.

Employees may:

- be held legally responsible for any liability associated with improper use
- be required to hand over the device in response to any investigation or legal proceeding
- be personally responsible for any costs associated with damage or misuse, if found to be due to negligence.

4. Compliance monitoring

Compliance monitoring will include:

- quarterly review of devices to ensure they still have operating system support
- monitoring of monthly call usage for exceptions
- monitoring of monthly data service usage for exceptions.

5. 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):

- Acceptable Use of Information and Communications Technology Policy
- Information Security Policy
- Microsoft 365 Acceptable Use Guidelines

6. Definitions

The following definitions are relevant to this policy.

Term	Definition
Mobile and data services	Access to telecommunication and internet services for mobile devices to be used for communication and data processing.
Mobile device	Portable electronic equipment that can connect to the internet, such as smartphone or tablet.
Data	The term 'data' generally refers to unprocessed information, while the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it.
Data service	Service purchased from third-party provider enabling connection to the internet over a wireless cellular connection.
Jailbroken or rooted device	Where software restrictions put in place by manufacturers to enhance data and information security have been removed from the device, e.g. to allow the installation of unauthorised software.
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.

7. 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 2022	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.