Government of Western Australia
Department of Health

Policy Frameworks
MP 0066/17
Effective from: 18 February 2021

Acceptable Use of Information and Communications Technology Policy

1. Purpose

The Acceptable Use of Information and Communications Technology (ICT) Policy sets out the acceptable behaviour required by staff, including contract and third party providers, across the WA health system when using WA health system ICT resources. For the purposes of this policy WA health system ICT resources includes, but is not limited to, ICT network, infrastructure, applications, portals, cloud, mobile devices, internet, storage, email, telecommunications, printers, faxes, photocopiers and video conferencing equipment.

The purpose of this Policy is to:

- outline the general obligations and responsibilities of staff in relation to the acceptable use of ICT resources across the WA health system, including reasonable personal use
- prevent misuse of ICT resources and minimise risk associated with unethical behaviour
- describe the access, monitoring and record keeping of ICT resources required by staff
- identify the consequences of breaching this Policy.

This Policy is a mandatory requirement under the *Information and Communications Technology Policy Framework* pursuant to section 26(2)(k) of the *Health Services Act 2016.*

This Policy is also a mandatory requirement for the Department of Health pursuant to section 29 of the *Public Sector Management Act 1994*.

This Policy supersedes the *Acceptable Use Policy* OD 0468/13, *Electronic Messaging Policy* OD 0469/13, *Email Management Policy* OD 0470/13, *Mobile Computing Devices Policy* OD 0336/11 and the *Mobile Telephone Policy & Guidelines* OD 0337/11.

2. Applicability

This Policy is binding upon all Health Service Providers, the Department of Health (known hereafter as 'the Department') and their staff.

In addition, Health Service Providers and the Department must ensure that in contracting with Contracted Health Entities, the entity and any of their personnel accessing the WA health system comply with all relevant mandatory requirements listed in this policy. This includes any person working in a permanent, temporary, casual, contracted, termed appointment or honorary capacity.

3. Policy requirements

3.1 General obligations and responsibilities for the use of ICT resources

All staff must ensure they use ICT resources in a professional, responsible and ethical manner[1]. Accordingly, and including but not limited to, ICT resources must not be used:

- to avoid established information security procedures
- for any unlawful, illegal, malicious or improper purpose
- to store, transmit, publish/display or communicate/distribute/post material which is obscene, defamatory, offensive, abusive, indecent, menacing, sexually explicit/oriented, threatening, or on the basis of race, religion, colour, age, sex, disability, ethnicity, sexual orientation, related to terrorist activities, illegal weapons, unwanted or otherwise unlawful or unauthorised or violates any law or regulation
- to knowingly transmit a computer virus or other malware
- in any way which improperly interferes with its availability for other users or otherwise interferes in the proper operation of the WA health system ICT resources/environment
- to access or damage another staff member's ICT resources without consent, regardless of whether or not such access or use has any adverse effects on the WA health system ICT network system, resources and data
- to infringe another person's intellectual property rights or release commercial in confidence material
- to disclose private or confidential data of another or look up data in a WA health system application regarding a relative, friend or person associated with any clinical incident, and not associated with purposes relating to your official duties
- to enable a minor to access material inappropriate for a minor or to establish (or attempt to establish) contact with a minor not otherwise known to you unless it is part of your official duties
- to harass or menace any person
- to conduct, maintain or promote a personal private business, use for profit or gain, including using WA health system ICT resources to assist relatives, friends or other persons in such activities
- to provide comments to journalists, politicians, lobby groups/activities, endorsement of products, outside fund-raising activities other than authorised in the course of your official duties
- to tarnish the reputation of the State of Western Australia, Department of Health or Health Service Provider, or claim to represent an entity within the WA health system when acting in a private capacity
- to interfere with any individual's reputation, employment or other obligations
- to send or receive bulk solicited email, collect or harvest email addresses of others for purpose of sending unsolicited emails or for sharing to external parties, or illegal activities, including peer-to-peer file sharing
- to create, send, or alter in any way the contents of emails for the purpose of hiding, obscuring or deleting the source of the message or making the message appear to come from someone other than the sender
- to breach any laws or infringe any third-party rights, or to breach any standards, content requirements or codes promulgated by any relevant authority or relevant industry body.

[1] *WA health Code of Conduct*, principles 1, 5 and 6

3.2 Reasonable personal use of ICT resources

Reasonable personal use of ICT resources is permitted by staff members where ICT resources are already provided for work purposes. Personal use of ICT resources are activities conducted for purposes other than accomplishing your official duties. In all cases, reasonable personal use must not result in loss of productivity, not interfere with official duties or not result in more than 'minimal additional expense' to the WA health system.

Staff must ensure reasonable personal use of ICT resources is not excessive outside of break periods.

Reasonable personal use of ICT resources may include where use may result in normal wear and tear, or small amounts of electricity, ink, toner or paper. For example this could include making only a few photocopies, using a printer to print out a few pages of material, making the occasional brief personal phone call, infrequently sending a personal email message, limited use of the internet or approved use of social media.

3.3 Minimise risk associated with misuse of ICT resources

Staff can minimise the risk associated with the misuse of ICT resources by:

- keeping passwords for WA health system ICT resources confidential
- not sharing passwords with other staff, and not using the logons and passwords of others
- changing passwords if anyone else may know them
- maintaining awareness of attempts by other parties to obtain passwords or other access credentials
- activating the screen saver or lock system if away from workstations
- logging out of systems when use is finished
- not sharing devices issued by a Health Service Provider or the Department with friends, family or non-approved staff members
- ensuring that devices issued by a Health Service Provider or the Department are not left in vehicles. Staff members are responsible for the security of the physical devices as well as the stored and accessed information. Individuals may be held liable for any negligence resulting in lost, stolen or damaged goods, or delay in reporting. Lost, stolen or damaged mobile devices should be reported to your line manager and Health Support Services as soon as possible. If stolen, a report should be made to WA Police to obtain an official report number for insurance purposes. For devices that are stolen and have remote disabling or erasure software installed, Health Support Services may erase all data on the mobile device, including private data. Health Service Provider or Department staff members using the device for storing private data do so at their own risk.

4. Compliance monitoring

Health Service Providers, the Department and Contracted Health Entities must develop internal processes to manage and monitor compliance with this Policy.

The System Manager, through Health Support Services, may require certain systems and the WA health system network to log transactions and communications whether private or business related.

Although systematic and ongoing surveillance of staff member emails and internet access logs will not occur, Health Service Providers, the Department and the System Manager through Health Support Services may monitor or investigate staff use of the WA health system ICT network systems and resources.

This will only occur to confirm compliance with the requirements of this Policy and to investigate possible incidents of breaches of security, unauthorised access or Human Resources matters.

A breach in confidentiality and security may be subject to disciplinary action and other remedies available through legislative provision such as the *Health Services Act 2016*, the *Public Sector Management Act 1994* and the *Criminal Code Act 1913*. Unauthorised access use and disclosure of confidential data, staff misconduct, including breach of this Policy is misconduct pursuant to the *WA Health Code of Conduct* and suspected cases may be reported to the Government of WA Corruption and Crime Commission.

5. Related documents

The following documents are mandatory pursuant to this Policy:

- N/A

6. Supporting information

The following information is not mandatory but informs and/or supports the implementation of this Policy:

- Microsoft 365 Acceptable Use Guidelines

7. Definitions

The following definition(s) are relevant to this Policy.

Term	Definition
Break periods	Times when staff are not otherwise expected to be addressing official business. Staff may, for example, use WA health system office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorised breaks, or weekends or holidays (if their work station is normally available at such times).
Confidentiality	The treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be used or divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission.
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. In this Policy the terms ‘data’

	and 'information' have been used interchangeably and should be taken to mean both data and information.
ICT resources	For the purposes of this Policy these include, but are not limited to, WA health system ICT network, infrastructure, applications, portals, cloud, mobile devices, internet, storage, email, telecommunications, printers, faxes, photocopiers and video conferencing equipment.
Information security	The practice of defending information/data from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
Minimal additional expense	Normal wear and tear or the use of small amounts of consumables.
Password	A secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many two factor authentication techniques rely on password as one factor of authentication.
Personal information	(As stated in the *Health Services Act 2016*) Has the meaning given in the *Freedom of Information Act 1992* in the Glossary clause 1: Means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead — (a)whose identity is apparent or can reasonably be ascertained from the information or opinion; or (b)who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.
Personal use	Activity that is conducted for purposes other than accomplishing official duties.
Staff member	As stated in the *Health Services Act 2016* (WA)), a staff member of a health service provider, means – (a)An employee in the health service provider (b)A person engaged under a contract for services by the health service provider. For the purposes of this policy, staff member also includes: (a)An employee in the Department of Health (b)A person engaged under a contract for services by the Department of Health.

8. Policy contact

Enquiries relating to this Policy may be directed to:

Title: Director, ICT Strategy and Governance

Directorate: Strategy and Governance Division

Email: ICTStrategyGovernance@health.wa.gov.au

9. Document control

Version	Published date	Effective from	Review date	Effective to	Amendment(s)
MP 0066/17	13 September 2017	13 September 2017	September 2020	18 February 2021	Original version
MP 0066/17 v2.0	18 February 2021	18 February 2021	December 2021	Current	Include Supporting information *Microsoft 365 Acceptable Use Guidelines.* Transition Policy to the current template.

10. Approval

Initial approval	Dr David Russell-Weisz, Director General, Department of Health
	28 August 2017
Current version approved	Nicole O'Keefe, Assistant Director General, Strategy and Governance Division, Department of Health
	15 February 2021

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