Government of **Western Australia**
Department of **Health**

Microsoft 365
Acceptable Use Guidelines

Table of Contents

1. Purpose

The purpose of this Guideline is to provide a practical guide for acceptable use of Microsoft 365 (M365) services by staff and contractors of the WA Health system. The Guidelines will:

- establish a context for M365 in relation to other information and communications technology services provided by Health Support Services;
- outline the general obligations and responsibilities of staff in relation to the acceptable use of M365 across the WA health system, including clinical use and reasonable personal use;
- define misuse of M365 and minimise risk associated with unethical or unacceptable behaviour; and
- describe the access, monitoring, information management and record keeping of M365 services provided to staff.

2. Applicability

This Guideline is applicable to all users of the WA health system licensed M365 product. This includes staff and contractors of Health Service Providers and the Department of Health. This includes any person working in a permanent, temporary, casual, contracted, termed appointment or honorary capacity.

3. Scope

The scope of these Guidelines includes:

- email services including mail, contact, calendars and tasks
- use of common M365 desktop services including Word, Excel, and PowerPoint
- use of collaboration services including online Word, Excel, PowerPoint, Teams (including Skype for business/Lync)
- storage services including OneDrive, Teams and SharePoint
- other applications within the M365 suite for which individuals have specific licences allocated e.g. Project, Visio, PowerBI, and
- additional apps within M365 such as Forms and Planner.

4. Responsibilities

All WA health employees and contracted staff are expected to follow these Guidelines whenever using M365, in order to comply with relevant policy and legislation.

Employees must at all times remember that when using M365, they are using a service provided to them for official business purposes.

The provision of M365 by Health Support Services is to improve productivity through the use of contemporary office technologies that afford greater mobility and efficient collaboration and communication between groups of staff. It is essential that the use of M365 is managed to ensure that it is used in an appropriate manner.

5. M365 context

5.1. Licensing and Management

M365 is a suite of application services provided by Microsoft Corporation Inc. under a whole of Government Enterprise Agreement (EA) license with Health Support Services on behalf of the WA health system.

M365 is a cloud-based service. The WA health system's partition of M365 is located in Australia and data within our in-scope applications are stored and transmitted within the Australian jurisdiction, when accessed within Australia.

5.2. Administration Responsibility

M365 is licensed as a Software as a Service (SaaS) and Health Support Services is responsible for the administration of the license and licensed administrative provisions.

Microsoft is responsible under the license for all Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) components underpinning M365.

Health Service Providers and the Department of Health are responsible for information management and usage concerned with the M365 service.

5.3. Security Controls

Health Support Services manages security and other administrative controls afforded under the Microsoft EA, ensuring compliance with the mandatory Information Security Policy (MP 0067/17).

5.4. Data Retention

Under the EA all data stored in M365 is retained by Microsoft while the EA remains valid. Files deleted by WA Health system employees are retained for seven (7) years and then permanently removed. Refer to section 6.4 for guidance on records management.

5.5. Access controls

Health Support Services manages access to the WA health system tenancy on behalf of the Health Service Providers and the Department of Health, and provisions access to M365 within licensing constraints and in adherence with all relevant policies.

M365 access is controlled and limited, in accordance with the following overarching principles:

- Need-to-Know and Need-to-Use principles: employees are only granted access to the information or information processing facilities they need to perform their tasks.
- Principle of Least Privilege: only the minimum privileges necessary to complete required tasks will be assigned to each employee.
- Employee access will be revoked after 90 days of inactivity, unless Health Support Services' Service Desk is advised of longer leave of absence.

Staff and customers of the HSS-provided M365 service need to align with these same principles, particularly in relation to the management of access controls associated with individual OneDrives and Teams collaboration capabilities.

5.6. M365 Cloud Zone

The WA Health Cloud Policy establishes three (3) zones for cloud computing, two (2) of which are applicable to M365:

Zone A – High Trust

This zone is designed, managed, and monitored by WA health, utilising all-of-WA-government service and support contracts. Centralised processes are in place to manage commissioning, billing, security, backups, business continuity and data privacy. WA State and Australian national legislation applies, making this the most trusted zone through which cloud services can be deployed.

Data stored in M365 is considered within Zone A. Accessing M365 is also considered within Zone A, when M365 is accessed via the WA Health network.

Zone B – Low Trust

This zone includes cloud services that are deployed by Third Parties within Australia and are therefore within Australian legal jurisdiction. However, services in this zone may be delivered via contracts that degrade patient or staff privacy, and are outside of any WA health managed security, backup, business continuity, or contractual management. Third Party staff supporting services in this zone maintain full and independent administrative access to any data hosted on their servers and are not covered under WA health employment terms and conditions.

Accessing M365 is considered within Zone B, when accessed via any non-WA Health network.

Zone C: Third Party Cloud – Offshore-Hosted (UNKNOWN Safety)

This zone is comprised of cloud services that may be hosted, staffed and backed up via any country. The legislative and contractual arrangements in these locations may significantly degrade patient or staff privacy and security, and in the event of an incident there may be no practical intervention possible from WA health, or any Australian legal or government entity. Data from services in this zone regularly spill via poor vendor practice or malicious attacks from the internet, making this the least trusted zone.

Accessing M365 from another country is considered to have unknown safety, including when accessed via VPN or Virtual Desktop in another country.

6. Related policies and legislation

6.1. General

This Guideline must be read in conjunction with:

- Digital Health Policy Framework
- *MP 0066/17 Acceptable Use of ICT Policy*
- *MP 0001/16 ICT Governance Policy (Patient Safety Risk Assessments)*
- *MP 0067/17 Information Security Policy*
- *MP 0140/20 Cloud Policy*
- Information Management Policy Framework
- *MP 0146/20 Information Classification Policy*
- *MP 0015/16 Information Access, Use and Disclosure Policy*
- *MP 0144/20 Information Retention and Disposal Policy*
- Retention and Disposal Schedule for Administrative and Functional Records
- *State Records Act 2000*
- *Freedom of Information Act 1992*
- *Health Services Act 2016*
- Other relevant WA health system or local Health Service Provider and Department of Health policies.

6.2. Legal Access to Information

Staff should be aware that all information in M365 products is subject to legislative provisions where official information can be requested. This includes:

- *Freedom of Information (FOI) Act 2004*
- Subpoena/Summons
- Orders to Produce
- *Coroners Act 1996*
- *State Administrative Tribunal Act 2004*
- *Health Services (Information) Regulations (Health Services Act) 2017*
- *Health Practitioner Regulation National Law Act 2010*
- *Parliamentary Commissioner Act 1971*
- *Criminal Injuries Compensation Act 2003* and
- *Children and Community Services Act 2004.*

6.3. Information Classification

It is a requirement of each WA health system employee to ensure that they manage information in accordance with *Information Classification Policy, Cloud Policy* and *Information Security Policy*, particularly where Official: Sensitive information (including personal, confidential or health information) is to be processed/transmitted.

The following table summarises secure handling of information on M365 and its associated information classification.

	Accessed From	Accessed Using	Storage	Information Classifications	Records Classification
Email	Health Network	Desktop Application	Exchange Online (M365 Cloud)	UNOFFICIAL OFFICIAL OFFICIAL: Sensitive	Ephemeral Limited personal use State Records must be stored in official records system, clinical application or business system.
	Other Networks	www.office.com	Exchange Online (M365 Cloud)	UNOFFICIAL OFFICIAL OFFICIAL: Sensitive	Ephemeral Limited personal use State Records must be stored in official records system, clinical application or business system.
Desktop Office Apps e.g. Word, Excel, Power Point, OneNote)	Health Network	Desktop Application	H: and W: Drive, Encrypted USB, OneDrive, Teams Folders, SharePoint	UNOFFICIAL OFFICIAL OFFICIAL: Sensitive	Ephemeral Limited personal use State Records must be stored in official records system, clinical application or business system.
	Other Networks	www.office.com	Encrypted USB, OneDrive, Teams Folders, SharePoint	UNOFFICIAL OFFICIAL OFFICIAL: Sensitive	Ephemeral Limited personal use State Records must be stored in official records system, clinical application or business system.
Collaboration Tools (e.g. Teams, SharePoint, and Online Office Apps)	Health Network	Teams, SharePoint, Desktop Application	H: and W: Drive, Encrypted USB, OneDrive, Teams Folders, SharePoint	UNOFFICIAL OFFICIAL OFFICIAL: Sensitive	Ephemeral Limited personal use State Records must be stored in official records system, clinical application or business system.
	Other Networks	www.office.com	Encrypted USB, OneDrive, Teams Folders, SharePoint	UNOFFICIAL OFFICIAL OFFICIAL: Sensitive	Ephemeral Limited personal use State Records must be stored in official records system, clinical application or business system.

EXPLANATORY NOTES

Information Classifications: These classifications are in line with the WA Government Information Classification Policy. Note this table does not include the classification *Commonwealth Security Classified*. In the event that any employee is required to handle this level of classification, they must refer to the secure handling requirements defined in the relevant inter-government agreement.

Networks:

> **Health Network**: includes onsite access at any WA health service or department (via direct cabled connections or internal Health Wi-Fi). Also includes VPN and Virtual Desktops.
>
> **Office.com** is considered a health network site as it is connected to the health network via a secure express routing method.
>
> **Other Networks**: includes home networks, secure mobile networks (not public Wi-Fi) within Australia. It is not recommended that M365 be accessed from overseas.

Official: Sensitive information may be emailed securely within the WA health system network. However, sending sensitive information by email should be undertaken with caution to prevent misdirection of patient information. Where possible, particularly where the information is very sensitive, the email should link to details hosted securely elsewhere (e.g. MyFT/ MyFX/ OneDrive/ SharePoint) so that it can be deleted when no longer needed.

Records Classifications: Refer to 6.4 for further information.

Teams Storage Files which appear to be saved in OneDrive and Teams Folders are stored in the M365 SharePoint platform.

6.4. Records Management

All information developed and stored in M365 is subject to the *State Records Act 2000*.

Employees can use M365 to create, organise and share information, as they would have done with traditional versions of Microsoft Office and network drives. If any of these documents can be defined as a State Record, employees must ensure that record is transferred and managed in the relevant records system. The record system can be an approved:

- record management system (such as TRIM or Objective) or
- business system (including corporate or clinical applications).

State Records are any form of information created, received or maintained by a government agency or parliamentary department in the course of conducting its business activities. State Records do not include ephemeral records.

State Records need to be retained in line with approved Record Keeping Plans and Retention and Disposal schedules.

M365 email, desktop and collaboration services may be integrated with the relevant records or business systems for direct transfer of information, when accessed from within the WA Health Network.

Ephemeral Records are records that are used to facilitate Government or State business but are of a trivial nature or used solely in the creation of more significant records. These records contain little or no ongoing administrative, fiscal, legal, evidential or historical value. Ephemeral records do not need to be saved into a recordkeeping system. Ephemeral Records can be destroyed once the need to access or reference them ceases. Examples of Ephemeral Records include:

- Extracts or exact copies of State Records, or other documents, circulars, forms, etc. where no annotations have been made.
- Externally produced information material, unsolicited letters or promotional material.
- Rough drafts of reports, correspondence, routine or rough calculations not circulated to other staff for comment / input, for which a final draft has been produced and placed on the appropriate subject file.

NOTE: Versions of drafts which contain major changes to content must be captured to the appropriate records subject file, e.g. internal policy.

6.5. Information Management

While M365 is not considered an information management system and is not suitable for storing State Records, information stored in applications such as Teams and OneDrive is still subject to policies and legislation as outlined in sections 6.1 and 6.2, and therefore must be planned and managed effectively to ensure it:

- can be valued and trusted
- is available and can be shared with anyone who may need it
- is secured and protected as needed, and
- meets policy and legal requirements.

To assist in meeting these objectives with Teams, it is recommended that Health Service Providers and the Department:

- Confirm the governance model for Teams including ownership, responsibilities and permissions.

- Adopt common definitions, formats and business rules, such as naming conventions for Teams names, files structures and documents (for example: State Records Office Document Naming Convention Guidelines).
- Establish any plans, policies, processes or procedures required, to ensure:
    - high quality information
    - appropriate information access or disclosure
    - information life cycle management (including record keeping and removal of any data that is no longer required, especially sensitive information)
- Provide further user training or user guides to optimise use of M365 services, maximise information sharing and reduce administration and risk. Some recommended uses are provided at Attachment A.

6.6. Clinical Use of M365

The use of M365 for clinical purposes can be an efficient mechanism for real time collaboration and communication, to support other systems of patient care. However, as with any new digital or paper-based process, patient safety, confidentiality and privacy must be foremost considerations.

Patient safety risks

Patient safety risks involving ICT are those that impact on having the correct information, correct patient and correct clinician, at the correct time and correct place. When considering the use of M365 for clinical purposes, patient safety risks must be assessed by the accountable clinician and clinical team involved.

The following example of good practice are provided for guidance:

- Clinician-to-Clinician Collaboration: A key decision, diagnosis or treatment decision discussed on Teams must be transferred to the patient's medical record.
- Clinical Teams Urgent Communication: All clinical team participants must be aware of Teams being used for urgent communication in order to manage patient prioritisation, and a timely response. Material communication must be placed on the patient's medical record.
- Real Time Documented Authorisation: A clinician may electronically approve medication for a patient while offsite using Teams and this authorisation must be placed on the patient's medical record.
- Clinical Teams Document Sharing: Clinical teams may share clinical guidelines or procedures (e.g. for the use of PPE or Clinical Pathways) via Teams or SharePoint, enabling team members greater access to these documents on any device and from anywhere.

Patient confidentiality or privacy risks

WA health system employees have a duty to maintain confidentiality about any personal or other information that becomes available to them in the course of their employment and to only use the information in connection with their role.

When using Teams for patient information, employees must ensure that they consider and manage any risks of this information being disclosed beyond its legal purpose.

An individual's consent to use or disclose information is required when the information is personal information and the use is unrelated to the use for which the information was initially collected.

An individual's consent to use or disclose information is not required when:

- the law permits or requires disclosure
- the information is not health information or another type of personal information
- the information is aggregated or statistical in nature
- the information is not reasonably identifiable, that is, contains no identifying information nor is able to be re-identified
- there is an overriding 'public interest' which justifies disclosure, such as to avert the threat of serious harm to individuals or to the public.

6.7. Remote Access and Security Risk Minimisation

M365 by its very nature is accessible from any location. Employees accessing M365 from home or other location that is not part of the WA Health ICT network, must:

- Protect their M365 account and password from disclosure.
- Use strong passwords and change passwords if anyone is suspected to know them.
- Maintain awareness of attempts by other parties to obtain passwords or other access credentials, such as via email or phone scams.
- Activate the screen saver or lock system if away from workstations or devices.
- Be wary of connecting to unknown or public Wi-Fi networks. Remain constantly aware that connections between the remote location and M365 provide a potential path to WA health system sensitive information.
- Be aware that all business electronic communication activities become WA health system property.
- Understand that they have the responsibility for the consequences should remote access be misused.
- Log out of M365 when use is finished.
- Notify the Health Support Services' Service Desk immediately if there is suspected theft or misuse of their remote access account.
- Don't share devices issued by a Health Service Provider or the Department with friends, family or non-approved staff members.
- Ensure that devices issued by a Health Service Provider or the Department are not left in vehicles or public spaces.
- Ensure that they have logged out of M365 on personal devices prior to sharing the device.

6.8. Reasonable Personal Use

MP 0066/17 Acceptable Use of ICT Policy describes acceptable use of all WA-health provided ICT equipment and systems. The following highlights its applicability to M365.

Reasonable personal use of M365 services is permitted by employees where M365 services are already provided for work purposes. Personal use of M365 services are activities conducted for purposes other than accomplishing 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. Employees must ensure reasonable personal use of M365 services is not excessive outside of break periods.

Reasonable personal use of M365 services may include storing a small amount of personal content in M365 OneDrive, incidental use of Outlook, Word, Excel, PowerPoint and other common applications.

6.9. Unacceptable Use

It is prohibited to create, send, access or store information that:

- Could damage the reputation of the WA health system.
- Involves or could lead to unlawful victimisation, discrimination, harassment or vilification.
- Is sexually suggestive, offensive, obscene, threatening, abusive or defamatory.
- Is used for operating a private business.
- Is deliberately misleading or deceptive.
- Is encrypted without the approval of your manager and does not comply with the WA Health encryption standards.
- Violates any State or Commonwealth law.
- Infringes copyright or other intellectual property rights.
- Impersonates another user, their M365 account or any other service.
- May hinder productivity (such as forwarding chain emails).
- May potentially destabilise WA Health systems or damage or impair information technology assets (e.g. sending a virus, downloading music/video.
- Is for unacceptable personal purposes (such as games, music, personal pictures and videos) other than what is permissible under reasonable personal use.

7. Monitoring and Compliance

Health Support Services has oversight of M365 including logging transactions and communications whether private or business related. Although systematic and ongoing surveillance of employee access to M365 will not occur, HSPs/DOH may monitor or investigate their staff use of M365. This will only occur to confirm compliance with the requirements of relevant Policy and to investigate possible breaches of security, unauthorised access, misconduct or other human resources matters.

A breach of the duty of patient confidentiality may lead to:

- disciplinary action by the employer or the health professional's regulatory body
- an action for damages against the person who made the unauthorised disclosure and/or his or her employer
- penalties, including fines, as specified in the *Health Services Act 2016* or other legislation as relevant.

A breach of discipline (e.g. if the employee contravenes a policy framework, commits an act of misconduct or is negligent in the performance of their functions) may be subject to Disciplinary Action in accordance with the *WA Health Discipline Policy MP 0127/20*, and other actions available through legislative provision such as the *Health Services Act 2016*, the *Public Sector Management Act 1994*, *Corruption, Crime and Misconduct Act 2003* and the *Criminal Code Act 1913*.

Attachment A: M365 Main Uses

	Suggested Uses	Tips
Teams	Directorate Clinical team Function, cross-function Project team	Where possible, avoid creating new Teams. Use existing Teams and ask Team Owners to add specific channels for your new purpose. Create a new Team when there is no existing team. Ensure the Team is created as a 'Private' team so that you may control visibility and access to the team. Ensure there are processes in place to ensure only members who require access to the team have access and review membership of the team regularly All records must be saved in an official records system.
Channel	Topics that the Team wishes to collaborate on	Consider using a Channel to divide the Topics collaborated on by the Team. Folders, files and other information can be stored and accessed for specific topics in this way. All records must be saved in an official records system.
Private Channel	Confidential topics for collaboration on by a few team members.	Create a private channel to collaborate on a confidential topic with a subset of Team members.
Chat	1:1 conversations Team conversations	Use Chat as a more efficient method for short communications and gestures. Be aware of holding group conversations in Chat that would be better suited to a Channel, which allows for greater visibility including by new team members. If considered a record, export the Chat and save it in an official records system.
OneDrive	Personal folder and file management similar to H: Drive.	Employees are responsible for managing access to files stored in their WA Health OneDrive. Avoid using OneDrive if documents should be shared more widely. All records must be saved in an official records system.
SharePoint	Use to share documents with entire departments or organisation-wide. e.g. HealthPoint.	Communications areas within Health entities must be consulted regarding the creation and use of SharePoint sites. SharePoint is typically used for the one-way broadcast of information such as news announcements, policies/guidelines, publications, templates and forms.