Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

Information Technology (IT) User Agreement Policy

Document Information	
Document Title:	Information Technology (IT) User Agreement Policy
Version:	PL2025-08-1.0
Category:	Corporate – Information, technology and communications
Approval for use details:	Owner: Executive Manager Corporate Services Approved by: Board Endorsed by: Executive Leadership Team Date approved for use: September 24 2025 Date due for internal review: September 25 2028
Purpose:	This policy sets out the conditions of use for all Information Technology (IT) systems, equipment, and digital resources at Katherine West Health Board Aboriginal Corporation (KWHB). It ensures staff, contractors, and volunteers use IT systems responsibly, securely, and in a way that supports high-quality health care and respects the values of our Aboriginal community.
Related Policies and Procedure/s:	1. Communications Policy 2. Cyber Security Policy 3. ICT Network Outage Procedure 4. Media and Public Relations Policy and Procedure 5. Photo, Video and Audio Policy and Procedure 6. Privacy and Confidentiality Policy and Procedure 7. Social Media Policy 8. Telehealth Policy and Procedure 9. Worker Accommodation Occupancy Agreement
Related Form / Document:	1. N/A
Key Word/s:	Information Technology (IT), Acceptable Use, Cybersecurity, Confidentiality, Privacy and Data Protection
External References:	1. Privacy Act 1988 (Cth) – Australian law governing how personal information is collected, used, stored, and disclosed. 2. Australian Privacy Principles (APPs) – Guidelines under the Privacy Act 1988 for handling personal information.

Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

	3. Australian Cyber Security Centre (ACSC) – Guidance on cyber security, including the Essential Eight Maturity Model: https://www.cyber.gov.au/ 4. Australian Digital Health Agency (ADHA) – Resources on secure digital health, My Health Record, and privacy: https://www.digitalhealth.gov.au/ 5. Office of the Australian Information Commissioner (OAIC) – Guidance on privacy and data protection: https://www.oaic.gov.au/ 6. Australian Commission on Safety and Quality in Health Care (ACSQHC) – National safety and quality standards, including clinical information systems: https://www.safetyandquality.gov.au/ 7. Stay Smart Online (ACSC initiative) – Practical guidance on safe online behaviours: https://www.staysmartonline.gov.au/ 8. eSafety Commissioner – Training and resources for safe technology use, including online behaviour and digital respect: https://www.esafety.gov.au/

Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

Background

Katherine West Health Board (KWHB) delivers health services across remote Aboriginal communities, where the use of Information Technology (IT) systems plays a vital role in supporting safe, effective, and culturally respectful care. IT systems are used daily to manage patient records, enable telehealth, support communication between staff and stakeholders, and protect sensitive information.

The increasing reliance on digital systems also brings responsibilities. Staff, contractors, students, and volunteers must use IT resources in ways that protect patient privacy, safeguard organisational data, and respect the cultural values of the communities we serve. This includes compliance with relevant Northern Territory and Australian laws, national privacy standards, and KWHB's own policies and cultural security framework.

The IT User Agreement provides clear expectations on acceptable use of IT systems. It is designed to:

- Support safe and secure handling of sensitive health information.
- Promote respectful and culturally appropriate digital communication.
- Protect KWHB systems from cyber threats, misuse, and unauthorised access.
- Ensure resources are used efficiently and for legitimate business purposes.
- Build community trust by demonstrating accountability, integrity, and professionalism in the use of digital technologies.

By following this policy, all users contribute to the safe delivery of healthcare services, the protection of client and organisational information, and the ongoing trust and wellbeing of the communities supported by KWHB.

Scope

This policy applies to all staff, contractors, students, and volunteers who access or use:

- Computers, laptops, tablets, and mobile devices
- Internet, email, and messaging systems
- Electronic Health Records (EHR) and other clinical systems
- Telehealth platforms
- Network and Wi-Fi services, including KWHB Wi-Fi provided in offices, clinics, and worker accommodation
- Software, databases, and cloud-based applications
- Any other digital resource owned, provided, or supported by KWHB

Use of KWHB Wi-Fi is subject to this IT User Agreement, the Cybersecurity Policy, and the Worker Accommodation Policy. Wi-Fi is provided to support legitimate business use and, in the case of accommodation, limited personal use is permitted, provided it:

- Does not interfere with work responsibilities or network security.
- Does not breach the Cybersecurity Policy or IT User Agreement.
- Respects cultural, legal, and professional standards, including prohibitions on accessing illegal or inappropriate content.

Closed Circuit Television (CCTV) and Surveillance Devices

- • The installation or use of Closed-Circuit Television (CCTV) or any other surveillance devices in KWHB staff accommodation is strictly prohibited unless prior written approval has been granted by KWHB management. Approval will only be considered where there is a demonstrated legitimate purpose consistent with organisational policies, safety requirements, and relevant Northern Territory legislation, including the *Surveillance Devices Act 2007 (NT).*
- • Staff are not permitted to install or operate personal CCTV, video doorbells, or similar surveillance equipment within or around KWHB accommodation without such approval. Any unauthorised devices must be removed immediately on request by KWHB and, in all cases, must be removed upon vacating the premises, regardless of the length of stay.
- • Any surveillance conducted without appropriate approval may constitute a breach of privacy under NT law and may result in disciplinary action, termination of accommodation privileges, and/or legal consequences.

Definitions

Term	Definition
Acceptable Use	Using IT systems responsibly, legally, and in line with KWHB policies and procedures.
Confidential Information	Any personal, health, or organisational information that is private and must not be shared without proper authorisation.
Cultural Security	A commitment to ensuring IT systems and communication respect Aboriginal cultural values, knowledge, and practices.
Data Breach	When personal, health, or organisational information is lost, accessed, disclosed, or used without authorisation (e.g., through hacking, accidental sharing, or theft).
Inappropriate Use of IT	Inappropriate use of the organisation's information technology (IT) resources includes any activity that is unlawful, unethical, or inconsistent with organisational policies, procedures, and values. This encompasses, but is not limited to: • Accessing, storing, transmitting, or distributing offensive, discriminatory, harassing, or sexually explicit material. • Using IT systems for personal gain, unauthorised commercial activities, or non-work-related purposes that interfere with productivity. • Downloading, installing, or using unlicensed, malicious, or unauthorised software or applications.

Term	Definition
	• Circumventing security controls, attempting to gain unauthorised access to systems, networks, or data, or disclosing confidential information without authorisation. • Misusing organisational email, messaging, or internet services to send spam, offensive communications, or information that could damage the organisation's reputation. • Excessive use of social media, streaming services, or other non-work-related sites during work hours. • Any activity that compromises the security, integrity, or performance of the organisation's IT infrastructure.
Malware	Malicious software (such as viruses or spyware) designed to damage or gain unauthorised access to IT systems.
Monitoring	The process of overseeing IT systems to ensure security, detect misuse, and protect organisational data.
Personal Information	Information about an individual that identifies them, such as name, address, date of birth, or health records.
Privacy	The right of clients, staff, and community members to have their personal and health information protected from unauthorised access or disclosure.
Telehealth	The use of video, phone, or digital technologies to provide healthcare services to clients in remote communities.
Unauthorised Use	Any use of IT systems, resources, or information that is not approved by KWHB or that breaches laws, policies, or cultural protocols.

Principles

1. **Confidentiality and Privacy** Protecting patient information and organisational data is essential to maintaining trust within our community.
2. **Cultural Respect** Technology must be used in a way that respects Aboriginal culture, values, and community protocols.
3. **Integrity and Accountability** Users are responsible for their actions and must use IT systems honestly, ethically, and transparently.
4. **Equity of Access** IT resources are provided to support all staff in delivering safe, effective, and culturally appropriate health care.

5. **Security and Safety** Protecting systems from cyber threats, misuse, and unauthorised access is critical to safeguarding community health information.
6. **Appropriate Use** IT resources are primarily for professional and health service purposes, ensuring the best outcomes for patients and the community, Respects cultural, legal, and professional standards. Recreational use of internet is permitted outside work hours in staff accommodation providing it:
    a. Does not interfere with work responsibilities or network security.
    b. Does not breach the Cybersecurity Policy or IT User Agreement.
    c. Respects cultural, legal, and professional standards, including prohibitions on accessing illegal or inappropriate content.
7. **Continuous Improvement** The organisation is committed to training, awareness, and adapting IT systems to meet evolving health care and community needs.

Responsibilities

The organisation (KWHB) will

- Provide secure, reliable, and culturally appropriate IT systems to support service delivery.
- Ensure compliance with all relevant Northern Territory and Australian legislation, including the Privacy Act 1988, My Health Records Act 2012, and data breach notification requirements.
- Develop, maintain, and review IT policies, procedures, and training materials.
- Promote cultural security and respect in the use of digital systems and communications.
- Protect client, staff, and organisational data from unauthorised access, misuse, and cyber threats.

The Board will

- Oversee governance of IT use, data protection, and cyber security at a strategic level.
- Ensure policies reflect best practice, legal requirements, and cultural security principles.
- Monitor organisational compliance with IT governance and risk management frameworks.
- Hold the CEO accountable for the implementation of IT user agreements and cyber security practices.

The CEO will

- Ensure organisational compliance with this IT User Agreement Policy.
- Allocate resources for IT infrastructure, security, training, and monitoring.
- Appoint appropriately qualified staff or external providers to manage IT systems and security.

- Report IT risks, breaches, and compliance issues to the Board.
- Promote a culture of accountability, cultural respect, and safe digital practices across the organisation.

Managers will

- Ensure staff, contractors, students, and volunteers under their supervision comply with this policy.
- Provide guidance and support to staff in the safe and appropriate use of IT systems.
- Monitor usage and report suspected misuse or breaches to the CEO or IT support.
- Support staff training in digital security, privacy, and cultural safety.
- Enforce disciplinary measures where breaches of the IT User Agreement occur.

Staff members will

- Protect the confidentiality, integrity, and security of patient information and organisational data.
- Use IT systems in a lawful, ethical, and culturally respectful manner.
- Comply with this policy, as well as relevant legislation (e.g., Privacy Act 1988, Health Records Acts, and the Notifiable Data Breaches scheme).

Legal Considerations

KWHB and all users of its IT systems have obligations under Northern Territory and Australian law. The following legal frameworks must be complied with at all times when using KWHB information technology systems and handling client or organisational information:

Privacy Act 1988 (Cth) Establishes the Australian Privacy Principles (APPs), which govern how personal, and health information is collected, used, stored, and disclosed.

Health Records and Information Privacy legislation (NT) Sets requirements for the protection and handling of health information in the Northern Territory.

My Health Records Act 2012 (Cth) Regulates the use, access, and protection of information in the national My Health Record system.

Notifiable Data Breaches (NDB) Scheme Requires KWHB to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) if a data breach is likely to result in serious harm.

Work Health and Safety Act 2011 (NT) Imposes a duty of care to ensure the health, safety, and wellbeing of staff and clients, including digital practices that protect against harm.

Fair Work Act 2009 (Cth) Ensures that workplace conduct, including online interactions, complies with employment law.

Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

Child Safe Standards and the *KWHB Child Safe Code of Conduct* Require staff to ensure safe and appropriate use of IT systems when working with or around children.

Criminal Code Act 1995 (Cth) Contains offences relating to unauthorised access, modification, or impairment of data and electronic communications.

Telecommunications Act 1997 (Cth) Governs the use of telecommunications systems and protection of communications.

Intellectual Property Laws (Copyright Act 1968) Protects the use of software, digital content, and online materials from unauthorised copying or distribution.

Document Modification History:	1. Created August 2025

**Any printed or saved documents from the document library may not be reflective of the current version. Check the document library for the most current version.*

Acknowledgement

It is a condition of employment that staff members acknowledge this IT User Agreement upon commencement and agree to the requirements. Digital acknowledgement in the Human Resource System is also required for revised versions of the Policy.

IT User Agreement

I will:	• Adhere to the Jirntangku Miyrta Enterprise Agreement, the KWHB policies and procedures, and all relevant NT and Australian Government laws and regulations relating to IT use, privacy, and cybersecurity. • Maintain confidentiality and privacy of all client, staff, and organisational information, ensuring digital data is only accessed, stored, or shared as authorised and in compliance with the Privacy Act 1988 and KWHB policies. • Use KWHB IT systems (computers, email, internet, electronic medical records, telehealth, mobile devices, software, and cloud services) responsibly and for legitimate business purposes. • Protect my login details and passwords, and immediately report any suspected misuse, security breach, or loss of data or devices. • Lock or log out of devices when unattended to prevent unauthorised access. • Respect and uphold the KWHB Cultural Security Framework in all digital communications, ensuring cultural sensitivity when using IT systems, including telehealth and online interactions. • Act honestly and professionally in all digital communications, including email, telehealth, messaging, and online collaboration platforms.

	• Use social media responsibly, upholding KWHB values and professional standards, including maintaining patient confidentiality, avoiding misleading claims, and ensuring that online conduct does not harm the organisation's reputation. • Complete required training in IT security, data protection, and cultural awareness as directed. • Report any suspected misuse of KWHB IT assets or systems (e.g., unauthorised access, inappropriate use of devices, or breach of privacy) to management or IT support.
I will not:	• Share my login credentials, access another person's account, or attempt to bypass security controls. • Use KWHB IT resources (including internet, email, and devices) for illegal, unethical, or prohibited purposes, such as harassment, discrimination, gambling, or unauthorised surveillance. • Store, copy, or transfer patient or organisational data onto personal devices, USBs, or unapproved cloud platforms. • Engage in cultural appropriation or misuse of Aboriginal cultural practices in online or digital contexts. • Post or share patient information, internal workplace matters, or culturally sensitive content on personal social media accounts. • Use offensive, aggressive, or discriminatory language in any form of digital communication, including emails, chats, and telehealth interactions. • Download, install, or use unauthorised software, apps, or files that may compromise KWHB systems. • Waste IT resources through excessive or careless use (e.g., unnecessary printing, streaming, or excessive bandwidth consumption). • Allow personal interests or relationships to influence IT-related decision-making or access to information. • Ignore or conceal instances of suspected IT misuse or data breaches. • Access, store, transmit, or distribute offensive, discriminatory, harassing, or sexually explicit material. • Use IT systems for personal gain, unauthorised commercial activities, or non-work-related purposes that interfere with productivity. • Download, install, or use unlicensed, malicious, or unauthorised software or applications. • Circumvent security controls, attempting to gain unauthorised access to systems, networks, or data, or disclosing confidential information without authorisation.

	• Misuse organisational email, messaging, or internet services to send spam, offensive communications, or information that could damage the organisation's reputation. • Excessively use of social media, streaming services, or other non-work-related sites during work hours. • Any activity that compromises the security, integrity, or performance of the organisation's IT infrastructure

If I think another person at KWHB has breached this IT User Agreement I will:

- Act to prioritise the best interests of staff members, clients and members of the public
- Take actions promptly to ensure that staff members, clients and members of the public are safe.
- Promptly report any concerns to my manager, the Chief Executive Officer, Board Director, or another manager or leader at KWHB.
- Follow KWHB policies and procedures for receiving and responding to complaints and concerns.
