Policy: Mobile Device and Wireless Connectivity Policy

Mobile Device and Wireless Connectivity Policy

Purpose

NSW Trustee and Guardian (NSWTG) has an increasing need to stay productive while on the move. Mobile device and wireless connectivity technology present a significant opportunity to improve access to information and ICT systems and therefore improve employee productivity.

The purpose of this policy is to provide direction to the proper deployment and use of all mobile End User Computing (EUC) devices (which include Laptops, Smart Phones, and Tablet Computers) by employees of NSWTG and Guest users. The policy also provides direction to staff about connecting to and using the wireless service provided by NSWTG. It is expected that all NSWTG staff, third parties, consultants and any other body authorised to use NSWTG information (hereby be referred to as NSWTG users) have an obligation to be aware of their personal responsibilities regarding appropriate and ethical use, information protection, confidentiality, and privacy.

Policy statement

- NSWTG IT will use mobile devices to support a flexible work environment to improve the efficiency and effectiveness of its workforce.
- NSWTG IT will issue mobile EUC devices in accordance with a standardised model for device allocations based on business need.
- NSWTG's Wireless Local Area Network (WLAN) connectivity is provided to approved users to enable mobility within NSWTG offices and branches. Wireless coverage within an office area will be appropriate to the security posture of the area. In certain high security areas wireless connectivity will be restricted.
- The WLAN service is the property of NSWTG which has the right to log, monitor and review use of the system.
- NSWTG IT Guest-Wi-Fi will support the use of 'Bring Your Own' (BYO) devices where it meets security and user obligations contained in this policy.
- Mobile device use is governed by NSWTG's policies and Code of Conduct.
- NSWTG IT has the right to monitor and review mobile EUC device usage for all NSWTG issued devices and approved 'Bring Your Own' (BYO) devices for NSWTG Guests.
- All, mobile EUC devices connecting to NSWTG's systems or networks must be configured to require:
    - User authentication prior to accessing the device.
    - Re-authentication after a defined period of inactivity

NSWTG issued mobile EUC devices:

- NSWTG provides mobile EUC devices to staff for official use. Private use must be restricted to incidental and limited use.

- All devices must be configured as per a standard operating environment (SOE) build.
- Streaming or downloading of video and audio over the mobile data network are limited to work related activities.
- Internet access over NSWTG's data network or the mobile data network is governed by the NSWTG's IT Acceptable Use Policy.
- NSWTG email access is governed by NSWTG's IT Acceptable Use Policy.
- Staff must follow instructions on updating device operating systems (OS) to the latest stable vendor issued release.
- Staff must not download or install unapproved/non-licensed software.
- Devices must not be hacked; jail broken or have their OS otherwise modified beyond the official vendor release.
- When directed by TAG IT, devices must be enrolled to use the Mobile Device Management (MDM) system - Microsoft Intune.
- Back-up of data stored locally on devices is the responsibility of the user. NSWTG assumes no responsibility for backing up locally stored data.
- Staff accept that NSWTG may remotely wipe the data or otherwise disable any device connected to information networks to protect NSWTG information and indemnifies NSWTG for the loss of any personal data that may result.
- Devices must not be left unattended in any location where theft is a possibility.
- If a device is lost or stolen, staff must immediately contact the TAG IT Service Desk. Staff must also report stolen devices to NSW Police and the incident reference number must be provided to the NSWTG IT Service Desk.
- Upon cessation of employment, it is the responsibility of staff to ensure that Mobile EUC devices and all associated peripherals are returned to their manager.

Personally Owned and Guest mobile EUC devices:

- NSWTG email access is governed by NSWTG's Email System Usage Policy.
- Except by written agreement, NSWTG will not provide support, advice or consulting for personally owned devices.
- Device owners are responsible for the security and protection of their devices and data stored on the device. NSWTG takes no responsibility for any damage to or loss of the devices.
- All costs associated with the use of a personally owned device will remain the sole responsibility of the device owner. Re-imbursement of costs for business related charges will only be considered where there is a specific written agreement in place with NSWTG, in advance of any claim.
- The owner accepts that NSWTG may remotely wipe only the data owned and/or managed by NSWTG, otherwise disable any device connected to NSWTG's email system to protect NSWTG information and indemnifies NSWTG for the loss of any personal data that may result.
- If a device that was connected to NSWTG's email system is lost or stolen, staff must immediately contact NSWTG IT Service Desk or tagit@tag.nsw.gov.au

CORP Wi-Fi - LAN Network Acceptable Use

- Wireless Intranet access connects corporate users wirelessly to corporate information assets. The access is provided to NSWTG IT approved devices ONLY. This may include TAG supplied laptop, tablet, smartphone or another specialist wireless device.
- The Acceptable use policy that applies to users accessing NSWTG information assets via the wired network is also applicable to the wireless network.
- Access to the corporate wireless network requires Active Directory login credentials and specific authentication protocols.

CORP Wi-Fi Guest Access Acceptable Use

- Where appropriate, NSWTG will provide limited, unsecured Internet access to guest users. The guests are required to register (self-service) and inform the guest ambassadors or contact NSWTG IT to get the access approved to connect to the guest wireless network. Guest Access will be time limited (based on business requirements); any extensions will be treated as a new access request. It should be noted that the speed and availability of guest Wi-Fi may not provide a reliable platform for hosting presentations or technical demonstrations by guests due to additional bandwidth and usage restrictions.
- Information transmitted via the guest wireless network may not be encrypted and may be viewed or intercepted by others. Privacy and security safeguards are the responsibility of the user – NSWTG assumes no responsibility for the security of this network. NSWTG does not warrant or represent that this service will be uninterrupted, error-free, or secure. Users should be aware that there are security, privacy, and confidentiality risks inherent in wireless communications and technology.
- NSWTG may monitor any activity or retrieve any information transmitted through this network, to ensure compliance with NSWTG's policy, and with federal, state, and local law. By accessing and using this network, you are consenting to such monitoring and information retrieval by NSWTG. Users should have no general expectation of privacy or confidentiality when using this network.
- This policy should be read in conjunction with the *NSWTG Privacy Policy* and *NSWTG Privacy Management Plan* which provide detailed information on how NSWTG manages personal, sensitive and health information.

Scope

This policy applies to all NSWTG Users. All mobile end user computing devices (NSWTG issued, BYOD and Guest) are covered by this policy.

Implementation

NSWTG is responsible for maintaining this policy and providing mobile EUC devices to approved NSWTG Users.

NSWTG ELT are responsible for circulating this policy in their respective divisions.

Managers and Supervisors should ensure that all staff are aware of this policy and have access to review its contents.

All staff are expected to comply with this policy. All staff are responsible for reporting any policy breaches to Managers and Supervisors in the first instance (or to division and executive heads, where necessary).

Legislative context

Government Sector Employment Act 2013

Workplace Surveillance Act 2005 No 47

Privacy and Personal Information Protection Act 1998

State Records Act 1998 No 17

Freedom of Information ACT 1989 No 5

Related resources

- IT Security Policy
- Data Privacy and Protection Policy
- Information Security Policy
- Access Control Policy
- Cloud Security Policy
- Code of Ethics and Conduct Policy
- Risk Management Policy
- IT Acceptable Use Policy
- M2002-04 Acceptable Use of the Internet and Email (Department of Premier and Cabinet)

Definitions

Term	Definition
Computing Device	Any electronic device which facilitates the storage, capture, transfer, use or creation of information.
Information Asset	Any information (both physical and digital in all formats, including audio and visual), application or ICT Configuration items (CI) which stores, transmits, creates or uses NSWTG information.
NSWTG	NSW Trustee & Guardian
NSWTG ELT	NSWTG Executive Leadership Team

Document information

Title:	Mobile Device and Wireless Connectivity Policy
Owner:	Mahendra Pardeshi
Approver:	David Watterson
Date of Effect:	20 September, 2022
Next Review Date:	20 September, 2025

Document history

Version	Date	Reason for amendment	Name/s
1.0	20/09/2022	Initial Draft Release	
2.0	15/05/023	Updated draft	Mahendra Pardeshi
3.0	17/05/2023	Legal & Privacy Team review (finalised)	Ruth Pollard, Hannah Muruste