Technology and Other Devices Policy and Guidelines

Current Version

Service Area	Disability, Aged, Community	**Version**	1.1
Process Owner	Governance Lead | IT	**Date of Issue**	Feb 2023
Approved by	Chief Executive Officer	**Review**	Feb 2025

Modification History

Version	Date	Author	Approved by	Description of change
1.0	5/2015	Natashia Telfer	Employsure	New policy
1.1	7/2021	Lisa Walker	Employsure	Additional separation of various devices in line with expansion

Contents

See Cyber Insurance Policy

See OPC Agreement

Technology, Phone and Other Devices

POLICY STATEMENT

Technology is a key factor in National daily operations across various internal and external sites. We are committed to safeguarding intellectual and physical property we may encounter, ensuring that it is managed in a manner that protects the security of all client and employee information access in line with the Privacy Act 1988, NDIS Quality and Safeguards Commission and the Ages Care Quality and Safety Commission.

SCOPE

All National employees and associates.

POLICY

- Identified point of contact for all National IT assistance.
- Identified "Agency" logins are implemented within facilitates for online documentation systems.
- Access to all National systems is limited and restricted to minimise risk of privacy breach and/or Cybercrime.
- CyberCrime Security Insurance is active across all identified National property.

Personal Mobile Phones

National have a zero tolerance for personal mobile phone usage during a rostered shift and/or work hours across service delivery unless in line with documentation requirements. Within management and administration respectful discretion is to be implemented. National do request in the event you do not have a work issued device, employees are expected to hold their personal mobile phone on their persons as a security measure. This ensures National can contact you and you can contact help in the event of an emergency. Phones are to be on silent and kept in your pocket. Within Community, phones can be utilised for client purposes including translator apps, and or eMims apps by the clinical team, Google Maps, CEIRA etc.

Employees are not to attempt to upload, download or acquire programs specific to National on their personal devices. National IT Security measures are in place and each device is required to be authenticated by NCC management.

No photos and/or recordings of any kind should be made without the expressed consent of National and the relevant parties. In the event this does occur to take photos of reportable incidents such as reports, property damage and/or client injuries (only with client consent), these images are to be sent to the appropriate up-lining person within National and promptly deleted from your personal device. General rule of thumb is if a photo needs to be taken, consent is required, and an incident report must be lodged within 24hours noting consent was gained.

Personal Devices

Personal mp3 players, iPod, and other personal devices should not be used during work time, other than in emergencies or on breaks. No photos and/or recordings of any kind should be made without the expressed consent of National and the relevant parties.

National and other Workplace Devices

General

The Employer phones, computers, laptops, iPads and other devices have been authenticated and to be used for business purposes and unless otherwise approved, strictly NO incidental personal use. Employees are to treat property with respect, maintain professional privacy for all National content and maintain basic upkeep of cleanliness.

Healthcare Settings may issue you with a facility phone (or keys) for your shift. It is expected property will be treated respectfully and returned at the completion of your shift. If an employee has a facility phone or device (or keys) and it is taken off site, it is the employees responsibility to return the phone or device immediately within their own time.

Accessing National Devices

- No employee is authorised to add their personal profiles and/or content to the National devices, and/or Cloud based storage under any circumstance.
- Employees requiring access to National Devices will be provided with said device and access codes at time of granted access.
- Initial access of any new National device that you have not previously been logged in to you will need to authenticate your login as a security measure. This should happen only the first time you login to that individual device.
- It will take approximately 10-15 minutes to download all your profile and settings from the cloud for you to access. Things such as large, shared email inboxes may not come up immediately and will take time to come in – be patient if you don't have them immediately.
- Logging in for the first time on a device may also require the authentication of our IT Admin – if you need authenticate and the authentication request screen comes up and you do not have the allocated phone device that can authenticate your profile, please call Matt on 0408797096 PRIOR to sending the authentication request so that we know to expect the request and can approve it immediately.
- If a request is not identified, the authorisation it will be declined for security reasons – ie is there someone trying to access our system that is not authorised to do so OR it may time out prior to us receiving the request and actioning it if we don't know the request is coming.
- Before logging in on any other computer device please sign out of any other computer you are logged in to – if you are changing workstations, sign out of the current one and login to the new one and give it a few minutes to load and sync.
- You do not need to sign out of your phone.
- Please make sure each device is signed out when not in use but left on – even the computers located out of the office. The IT admin and security provider of choice will run updates and maintenance on the devices overnight and continue monitoring security.
- All employee users are to save your work documents prior to finishing for the day and before signing out to avoid losing any work.
- Your device may require a restart and alert you to do so. Do not delay or reschedule the restart notification as it can cause profile issues and security vulnerabilities if update can not be finalised with the reset.
- No linking of personal devices to National devices and/or equipment is permitted

- See *National Online Security* below

Accessing Team National SharePoint

- Access to Team National SharePoint is delegated by National management and only available upon National authenticate devices to ensure the safety and privacy of information and data.
- Drives include National, Admin, Clients, Employees, Management, Templates, Bunbury, Clinical
- All documents accessed by employee should be accessed live OR checked out. Upon completing work on document, titled appropriately and saved in appropriate folders.
- Do not create duplicates of same document.
- All registers should not be checked out. Registers are to be used as LIVE version only.
- Depending on employee allocated security clearance will indicate level of access within SharePoint.

Directors	Administration	Clinical Team	Support Coord	SIL / Onsite
All drives	NCC* NCC Employees Admin	NCC*+ Clinical NCC Clients Employees Sites Templates	NCC* NCC Clients Templates	Sites NCC Clients (SIL) Templates

*limited access

Training portal IT Access

Please contact info@nationalcommunitycare.com.au

Non-Urgent Authenticated National Device Assistance

For non-urgent queries, email matt@nationalhealthcare.com.au to ensure appropriate actions can be taken safeguarding security across all devices.

When reporting IT concerns please provide as much information as possible so a diagnostic determination can be made. This may include the following:

- *What is occurring?*
- *What are you doing when it occurs?*
- *Have you reset the computer?*
- *Have you logged out and logged back in?*
- *Are there any pop-up notifications?*
- *Have you recently attempted to download or upload anything?*

Urgent IT Assistance

Urgent assistance is any IT concern you may experience that hinders your immediate ability to complete your work. This may include authenticating your device. If this is the situation, please call our contracted standby support - Matt on 0408 797 096 and have ready as much information as possible. There are some issues we will be able to resolve immediately, and some will require further investigation.

IT Systems Updates

To ensure National have exceptional resources available to our team, the National secure network, and Rostering Platforms STARS and CEDAR often require ongoing maintenance, security checks and software updates. These updates are usually scheduled for after business hours when possible. In the event an unavoidable disruption occurs, National will provide reasonable notice (if possible) of the system maintenance if it is suspected to disrupt daily operations including Management Systems access and Employee Systems access. Any IT concerns should be identified and reported to National immediately via matt@nationalhealthcare.com.au.

National Online Security

For security purposes, all documents should be labelled appropriately and securely stored on the appropriate National Drives. Common Drive, NHS Drive, NCC Drive, Support Coordination, Clinical Coord and Bunbury Drive. This allows shared access across all working sites with the most up to date version. Desktops should be kept from clutter with strictly NO original documents on desktops as it is not secure and can be lost in the event of a power outage or system reset/update. All employees are required to log out of profiles on desktops upon completion of tasks and are not to share login details.

Misappropriation of National Property

Any unauthorised personal use may be repayable by you and may result in disciplinary action up to and including termination. The Employer reserves the right to deduct the appropriate sums from your salary in the event that repayments are not made.

Client/participant Devices

Client/participant phones, computers, laptops and other devices are to be used for client/participant purposes only. Assisting client/participants with accessing their phones or other devices needs to be done respectfully and with client/participant permission.

Any unauthorised personal use may be repayable by you personally and may result in disciplinary action up to and including termination. The Employer reserves the right to deduct the appropriate sums from your salary in the event that repayments are not made. If an employee has a clients phone or device (or any other property belonging to the client) and it is taken off site, it is the employees responsibility to return the device immediately within their own time.