



4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

BC8.2 Mobile Device Data Usage Separation

Overview

NTPC enforces a bring your own device (BYOD) data model and grants all employees and contractors that have access to its systems to connect a smartphone or tablet (regardless of device ownership) to its systems and services. NTPC reserves the right to revoke this privilege if users do not abide by the details outlined below. This IT Policy is intended to protect the confidentiality, integrity and availability of NTPC's data and technology infrastructure. Limited exceptions to this IT Policy may occur due to variations in mobile devices and platforms. NTPC employees must agree to the terms and conditions set forth in this document in order to be able to connect their mobile devices to NTPC's systems and services.

Devices

The following are acceptable devices:

- Smartphones including iPhone and Android based devices are allowed.
- Tablets including iPad and Android are allowed.

Mobile Device Management (MDM)

1. NTPC uses the Microsoft Intune mobile device management solution to secure mobile devices and enforces technical management policies remotely. Before connecting a mobile device to NTPC systems and services, the mobile device must be set to be manageable by NTPC.
2. All devices, regardless of device ownership that are connected to NTPC systems and services must have the Microsoft Intune Company Portal installed. Assistance in finding and installing this application can be sourced via the helpdesk@ntpc.com support team.
3. The Microsoft Intune mobile device management solution enables NTPC to take the following action on mobile devices – restricted only to NTPC data: remote wipe of NTPC data, and remote lock of the NTPC data.
4. Any attempts to contravene or bypass the Microsoft Intune mobile device management implementation will result the mobile device being marked as non-compliant and all NTPC data will be wiped from the device.



4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

Personal/NTPC Data Separation

All mobile devices, regardless of device ownership, will use NTPC's implementation of Microsoft Intune if access to NTPC's systems and services is required/desired. This platform has a hard separation of NTPC's data from personal data.

These are the things that NTPC **can never see from Personal Data**

- Calling and web browsing history
- Email and text messages
- Contacts
- Calendar
- Passwords
- Pictures, including what's in the photos app or camera roll
- Files

Things that NTPC **can always see**

- Device owner (your NTPC username)
- Device name (such as "Susan's iPhone")
- Device serial number
- Device Model (such as "iPhone XR")
- Device Manufacturer (such as "Apple")
- Operating system version (such as "iOS 12.0.1")
- Device IMEI
- Application inventory names of only NTPC pushed apps (such as "Outlook" or "Authenticator")

The system is configured such that personal data can move into the NTPC side of the phone, but NTPC data cannot be removed and placed into the personal side of the phone. For example, you can attach a photo from the phone to an NTPC email, but you will be blocked from saving a photo attached to an NTPC email into the personal photo roll on the phone.



4 Capital Drive, Hay River, NT X0E 1G2 • Tel: (867) 874-5200 • Toll-free fax: 1-888-332-9640

These are things that NTPC **might be able to see** on your mobile device:

	Personally Owned Device	NTPC Owned Device Supplied to you
Phone Number	Only the last 4 digits	The full phone number
Storage Space	Total space and space available	Total space and space available
Location	Not available	Not available
Applications Installed	Only NTPC pushed apps	Only NTPC pushed apps
Subscriber Carrier	Yes (i.e. Bell, Telus, Kudo, etc.)	Yes (i.e. Bell, Telus, Kudo, etc.)
WiFi MAC	Yes	Yes
WiFi IPv4 Address	No	Sometimes
Encryption Status	Yes	Yes
Jailbroken Status	Yes	Yes

Review

This document and associated audit record is reviewed once every 12 months.

Version History

Version	Date	Description	Approved By
1.0	March 2, 2023	Initial version.	