Mobile Devices (iPhones)

Guides for PBR-issued iPhones — setup, security, approved apps, and policies.

- iPhones Issued to Individuals
- iPhones Issued to Roles
- Banned and Restricted Applications on PBR Devices

iPhones Issued to Individuals

Passcode and Verification Management

PBR issued Mobile Phones must be kept secure at all time.

The following tools can be used to increase your device security

- Change the provided passcode immediately
- Ensure a 6 digit passcode is kept on the device
- Biometrics - FaceID or TouchID may be used for convenience.
- Ensure a lock screen timeout is in place (recommended 3 minutes)

Linking your PBR account to the Phone

PBR issued Mobile Phones have the Company Portal app already deployed and installed. This app links your work account, and allows you to access PBR Services.

- Log into the Company Portal App as soon as possible. This will deploy your default applications
- Any applications which are required for your PBR job role are available to download within the Company Portal app.
  - If a specific PBR-required Application is not available within the Company Portal, please contact the PBR IT Helpdesk via email - helpdesk@pbr.org.au, to request the app be made available.

Personal Usage of PBR Issued Mobile Phones

As per the Mobile Phone Policy, reasonable personal use of issued Mobile Devices is permitted.

Applications that are installed for Personal Use, should be kept to a minimum as to not interfere with PBR duties, or affect the ability to use the Mobile Phone

To install Personal Applications:

- Sign into the device or App Store using a personal Apple ID, this is not related to your Work Email.
- There are a list of banned/prohibited applications, as mentioned in the Mobile Phone Policy, which are not permitted to be installed on PBR Mobile Devices under any circumstances. You can find this **here.**

General Personal Use Guidelines

- Ensure you are following the PBR Code of Conduct, Social Media Policy, and other relevant PBR Policies at all times when utilising a PBR Mobile Device
- International Roaming is not enabled on PBR Mobile Plans
- Excessive personal use of PBR Mobile Plans is not permitted, with excessive personal use costs to be reimbursed by the user.

Damage, Theft and Safe Use of PBR Mobile Phones

- All PBR Issued Mobile Devices are issued with a Case and Screen Protector. This is designed to Protect your device from accidental drops or falls.
- If a Screen Protector is broken, it is to be replaced as soon as possible.
- If your device is damaged, please immediately contact the PBR IT Helpdesk, who can organise repairs.
    - If this occurs as part of your work duties, ensure an Incident Defect Report (IDR) is submitted
- If your PBR Issued Mobile Device has been stolen or lost, you MUST inform the PBR IT Helpdesk and/or your Line Manager immediately.
    - All Stolen items must be reported to Law Enforcement Authorities, with a report obtained. This is required for Insurance Purposes, and is mentioned under the PBR Mobile Phone Policy

Monitoring and Logging and Acceptable Use

As per the Mobile Phone Policy, the provided device remains as PBR Property at all times, and as such, PBR reserve the right to monitor and audit all activity undertaken on the device.

- Ensure you have read, and are familiar with the PBR Mobile Phone Policy.
- Ensure you are following the PBR Code of Conduct, Social Media Policy, and other relevant PBR Policies at all times when utilising a PBR Mobile Device
- PBR Team Members are responsibly for exercising good judgement around usage of a PBR Mobile Device
- PBR IT reserve the right to remotely disable, wipe or modify your Mobile Device as required.
    - These actions will only be taken in extreme circumstances, and at the direction of the PBR IT Manager, Group Manager Business Services, or CEO.
- Not all settings or features will be available on your PBR Issued Mobile Phone.

iPhones Issued to Roles

Passcode and Verification Management

PBR issued Mobile Phones must be kept secure at all time.

The following tools can be used to increase your device security

- Change the provided passcode immediately
- Ensure a 6 digit passcode is kept on the device
- Ensure a lock screen timeout is in place (recommended 3 minutes)

Application's on Role Based iPhones

- Any applications which are required for your PBR job role are preinstalled on the device.
  - If a specific PBR-required Application is not available on your device, please contact the PBR IT Helpdesk via email - helpdesk@pbr.org.au, to request the app be made available.
- Personal Applications are not able to be installed on PBR Role Based iPhones.

Personal Usage of PBR Issued Mobile Phones

As per the Mobile Phone Policy, reasonable personal use of issued Mobile Devices is permitted.

General Personal Use Guidelines

- Ensure you are following the PBR Code of Conduct, Social Media Policy, and other relevant PBR Policies at all times when utilising a PBR Mobile Device
- International Roaming is not enabled on PBR Mobile Plans
- Excessive personal use of PBR Mobile Plans is not permitted, with excessive personal use costs to be reimbursed by the user.

Damage, Theft and Safe Use of PBR Mobile Phones

- All PBR Issued Mobile Devices are issued with a Case and Screen Protector. This is designed to Protect your device from accidental drops or falls.
- If a Screen Protector is broken, it is to be replaced as soon as possible.

- If your device is damaged, please immediately contact the PBR IT Helpdesk, who can organise repairs.
  - If this occurs as part of your work duties, ensure an Incident Defect Report (IDR) is submitted
- If your PBR Issued Mobile Device has been stolen or lost, you MUST inform the PBR IT Helpdesk and/or your Line Manager immediately.
  - All Stolen items must be reported to Law Enforcement Authorities, with a report obtained. This is required for Insurance Purposes, and is mentioned under the PBR Mobile Phone Policy

Monitoring and Logging and Acceptable Use

As per the Mobile Phone Policy, the provided device remains as PBR Property at all times, and as such, PBR reserve the right to monitor and audit all activity undertaken on the device.

- Ensure you have read, and are familiar with the PBR Mobile Phone Policy.
- Ensure you are following the PBR Code of Conduct, Social Media Policy, and other relevant PBR Policies at all times when utilising a PBR Mobile Device
- PBR Team Members are responsibly for exercising good judgement around usage of a PBR Mobile Device
- PBR IT reserve the right to remotely disable, wipe or modify your Mobile Device as required.
  - These actions will only be taken in extreme circumstances, and at the direction of the PBR IT Manager, Group Manager Business Services, or CEO.
- Not all settings or features will be available on your PBR Issued Mobile Phone.

Banned and Restricted Applications on PBR Devices

Overview

PBR-issued devices are managed through Microsoft Intune (Company Portal). Certain applications are prohibited on PBR devices for security, legal, or compliance reasons.

Prohibited Applications

Application	Reason
TikTok	Prohibited under Australian Government guidance due to security concerns — banned on all government-adjacent and critical infrastructure devices

This list will be updated as new guidance or policy changes arise.

Installing New Applications

If you need a specific app for your PBR role, contact IT Helpdesk. Do not install apps from outside the App Store, and do not use personal Apple IDs to install apps on PBR-issued devices.

IT can push approved apps directly to your device through Company Portal.

Accessing the App Store on a PBR Device

The App Store is available on PBR devices for personal app use within acceptable use policy. However:

- Do not use your personal Apple ID if the device was issued with a managed Apple ID
- Prohibited applications may be blocked or automatically removed by Intune policy
- Work-related apps should be installed via Company Portal, not the App Store directly