AFP National Guideline on mobile devices

1. Disclosure and compliance

This document is marked **For Official Use Only** and is intended for internal AFP use.

Disclosing any content must comply with Commonwealth law and the AFP National Guideline on information management.

Compliance

This instrument is part of the AFP's professional standards framework. The AFP Commissioner's Order on Professional Standards (CO2) outlines the expectations for AFP appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the *Australian Federal Police Act 1979* (Cth).

2. Acronyms

AFP	Australian Federal Police
AFPNet	Australian Federal Police Network
ICT	Information and communications technology
RSS	Rich Site Summary
SIM	Subscriber identity module
SMS	Short Message Service
T&I	Technology & Innovation

3. Definitions

Accessories – means the peripheral equipment issued with mobile devices. Accessories can be standard (e.g. protective cover, cables, battery, rapid charger and personal hands-free earpiece) or specialised (e.g. wearables).

Additional service – means any carriage service that is not a basic service (e.g. international roaming).

AFP appointee – means a Deputy Commissioner, an AFP employee, special member or special protective service officer and includes a person:

- engaged overseas under s. 69A of the *Australian Federal Police Act 1979* (Cth) (the Act) to perform duties as an AFP employee
- seconded to the AFP under s. 69D of the Act

engaged under s. 35 of the Act as a consultant or contractor to perform services for the AFP and determined under s. 35(2) of the Act to be an AFP appointee.

(See s. 4 of the Act.)

Approver – is a:

- team leader, coordinator or superintendent for band 1-8 AFP appointees
- manager or commander for band 9 AFP appointees.

The approver is not required to provide PGPA approval but is to ensure the Approval Process (Section 8) is followed.

Carriage service – means the service provided to allow the transmission of voice (voice calls) and data (SMS and internet) from the mobile device. Most mobile devices will require voice and data services except operational tablets and corporate laptops / tablet which will require data services only

Cloud – means cloud computing which is a type of Internet-based computing that provides shared resources, software and information to computers and devices on demand.

Container – is an authenticated, encrypted area on a mobile device used to insulate / protect corporate data from personal data or apps.

Custodian – means an AFP appointee issued with an AFP mobile device and/or SIM card.

Data spill – means when any classified information is introduced onto an ICT system which is not accredited to handle the information.

Inappropriate material – means material which must not be transmitted, loaded and/or stored on AFP ICT systems due to its illegality or effect on the AFP's reputation, security or operational effectiveness. It includes material that is:

- unlawful or fraudulent
- obscene, offensive or pornographic (offensiveness is judged against the AFP Core Values)
- harassing, racist or discriminatory
- sexist, defamatory or vilifying
- political, if anyone receiving the material could question the user's standard of service to any elected government.

Information – means AFP documentation which is created, received, used and/or maintained by the AFP regardless of physical or electronic form.

Mobile application – means a software application that runs on a mobile device that may access the internet.

Mobile device – is considered ICT equipment as it is a data storage device and if lost or damaged a Security Incident Report will need to be completed. There are three main categories of mobile devices for use in the AFP:

- **policing operations** – devices that are primarily designed and used for operational rather than administrative reasons. Types include:
  - smartphones (operational)

    - tablets (operational)
- **corporate access** - devices used to provide access to AFPNet or other corporate networks. Types include:
    - smartphones (AFP access)
    - laptops / tablet (corporate)
- **telecommunication** – devices primarily used for the purpose of SMS, voice calls, personal hotspot and limited internet/data access. Types include:
    - mobile phones
    - satellite phones
    - satellite terminals
    - modems.

Official use – means used for the purpose of addressing an AFP operational or business need.

Pool mobile device – means a mobile device which is available for shared use within a team or function of the AFP.

Personal use – means phone calls or data usage of a mobile device of a personal nature, not required for work purposes and not related to an emergency.

Reputable – means a network that a user could reasonably assume to be operated without malicious intent as the owner/manager can be considered trustworthy or is regularly used by other government agencies.

Satellite phone – is a type of mobile phone that connects to orbiting satellites instead of terrestrial cell sites. They provide similar functionality to terrestrial mobile telephones. Voice, SMS and low-bandwidth internet access are supported through most systems.

Satellite terminal – is a terminal normally used to connect a laptop computer to broadband Internet in remote locations, but can be used anywhere there is line-of-sight to the satellite. A terminal is about the size of a laptop and can be carried easily.

Security classified information – includes data with any security classification, dissemination limiting marker or caveat.

Smartphone (AFP access) – is a device that, additional to normal telephony functions, is capable of accessing a range of AFP corporate systems (including email & calendar) and storing data up to a classification of PROTECTED. They can also provide a Wi-Fi hotspot function for other devices. These devices have access to use a variety of accessories that enable convenient or covert use.

Smartphone (operational) – is a device designed specifically for operational use (e.g. ruggedised with extended battery life). They have the ability to access a range of AFP corporate systems (including email & calendar) and provide inbuilt Push-to-Talk and duress capabilities. These devices have access to use a variety of accessories that enable convenient or covert use.

Tablet / laptop (corporate) – is a device configured to provide general corporate remote access. They are reasonably light for easy portability, but also act as a desktop when used in conjunction with a docking station.

Tablet (operational) – is a device designed specifically for operational mobile use so they are generally smaller than a corporate tablet device but bigger than a smartphone for easier data entry and capture. The device can be ruggedised and designed for niche use (e.g. in-car

computing).

Use – means SMS, voice calls and internet/data access whether domestic or international, as well as accessing the functionality on the device such as mobile applications.

Wearables – means smart electronic devices (electronic device with microcontrollers) that can be worn on the body as an implant or accessory. The designs often incorporate practical functions and features. Common types include smart watches, activity trackers and health monitoring vests.

4. Guideline authority

This guideline was issued by the National Manager Technology & Innovation using power under s. 37(1) of the *Australian Federal Police Act 1979* (Cth) as delegated by the Commissioner under s. 69C of the Act.

5. Introduction

This guideline details AFP appointees' obligations when obtaining, managing and/or using official mobile devices and relevant carriage services.

It should be read with the:

- Commissioner's Financial Instructions
- AFP National Guideline on procurement and contracting
- AFP National Guideline on the security of ICT hardware and software
- AFP National Guideline on the security of information systems
- AFP National Guideline on the security of ICT system access
- AFP National Guideline on the security of removable data storage devices.
- AFP National Guideline on information management.

6. Using AFP mobile devices

Custodians must:

- protect the security and integrity of the mobile device as per the AFP National Guideline on the security of information systems
- use mobile devices in an acceptable manner in accordance with this guideline
- ensure equipment is protected against theft, unauthorised access, compromise, illicit use, unauthorised modification or intentional damage
- report any loss or damage via a Security Incident Report (see s. 18)
- securely manage official information obtained through the use of a mobile device, as per the AFP National Guideline on information management.
- ensure the safe custody of equipment until it is:
  - formally transferred to another AFP appointee via the asset transfer process within Insight!
  - returned to the issuing authority
  - returned to the nominated AFP team (see s. 18) for final disposal.

This guideline observes obligations under the:

- Australian Government Information Security Manual
- Australian Government Protective Security Policy Framework
- AFP Commissioner's Order on Security (CO9)
- AFP National Guideline on the security of information systems.
- AFP National Guideline on the security of ICT system access.

If an AFP appointee intends to use a mobile device internationally they must do so in accordance with the AFP National Guideline on travel and living away from home.

For further advice on the secure use of mobile devices in international locations, contact Security Reporting and Referrals.

7. Procurement of mobile devices

All mobile devices must be purchased via Department of Finance established Whole of Australian Government arrangements.

In the unique situation where an approved mobile devices cannot be procured via this process the device must be purchased in accordance with the Commonwealth Procurement Rules.

Business areas are able to purchase all mobile devices types through T&I (see T&I Contact Us page, http://serviceportal.afp.le/ or call 02 6131 4666, x146666).

Note: Accessories and wearables will generally be available to be purchased with the device but if individual/additional items are required it is more cost effective for an individual to purchase the accessories directly from a store using their corporate credit card (subject to normal financial processes and approvals within their section).

8. Approval process

Before endorsing a request for a mobile device, including purchasing additional services, an approver must:

- ensure the requested mobile device aligns with the device allocations linked with job roles in the Job Family Model (a forthcoming list of the device allocations will be published on the AFP Hub)
- ensure the requester does not already have the maximum number of devices assigned to their Job Family role
- consider security, integrity and privacy issues associated with using mobile devices and utilisation of additional services.

Exceptions to this must be endorsed at National Manager level.

9. Official use

Except where there is an overriding operational and/or business need, AFP appointees must use AFP systems (e.g. AFP radio communications, AFP corporate voice systems, AFP mobile devices or AFP computer systems) when conducting official business communications.

AFP mobile devices must be used in accordance with the values and conduct expectations in the

AFP Commissioner's Order on Professional Standards (CO2).

10 Prohibited use

AFP appointees must not, without lawful excuse or authority, use AFP mobile devices:

- in a way that could adversely impact the AFP
- for personal gain, including any personal business interest even if it is approved secondary employment
- to create, access, distribute or store inappropriate material
- to access non-AFP ICT systems or data that could endanger the security of AFP ICT systems, including:
  - seized or intercepted computer data which has not been appropriately sanitised (e.g. by Digital Forensics)
  - known malicious software or viruses
  - untrustworthy websites or files
  - unapproved hardware.

If inappropriate material has been unintentionally accessed by legitimate searches, or the nature of material was not evident from the title or link displayed, AFP appointees must:

- immediately exit the inappropriate material
- make a file note or diary entry describing the circumstances
- notify their supervisor
- submit a Security Incident Report to Security-Reporting-and-Referrals@afp.gov.au, in accordance with the AFP National Guideline on security reporting.

Unauthorised, unacceptable and/or inappropriate use of an AFP mobile device must be reported in accordance with the obligations in the AFP Commissioner's Order on Professional Standards (CO2) and the AFP Commissioner's Order on Security (CO9). This use includes, but is not limited to:

- installing, using or viewing inappropriate material including inappropriate ring tones, pictures or applications
- sending, displaying or broadcasting any content amounting to unlawful disclosure, discrimination, sexual harassment or bullying.

11 Call forwarding/diverting

AFP desktop phones must not be diverted to personal mobile devices unless authorised in writing by an approver. If available, an 'out-of-office' voicemail should instead be recorded including the mobile device number.

12 International roaming

International roaming may be enabled on a mobile device carriage service when travelling outside Australia if approved by the AFP appointee's manager or commander.

Approved requests for international roaming must be sent for action to T&I (see T&I Contact Us page, http://serviceportal.afp.le/ or call 02 6131 4666, x146666).

Unless required for operational reasons, custodians must deactivate all internet connectivity to avoid incurring additional costs including, but not limited to:

- RSS feeds
- automatic syncing for background data
- data roaming
- push email
- syncing of non-essential data using the mobile network
- geolocation services.

13 Wi-Fi

Public and privately operated Wi-Fi networks may be used where appropriate and where the network operator is understood to be reputable. Information which is not secured or controlled by an approved enterprise management tools could be intercepted by malicious persons, therefore AFP appointees must use caution when joining public Wi-Fi access points.

AFP appointee using a Wi-Fi network in an international location must adhere to the AFP National Guideline on travel and living away from home. For further advice on the secure use of mobile devices in international locations, contact Security Reporting and Referrals.

14. Personal use

Personal use must be in accordance with the AFP National Guideline on the security of information systems.

AFP appointees are entitled to reasonable personal use of AFP-issued mobile devices; however, standard AFP corporate processes including monitoring and reporting of data usage will occur.

When assessing whether usage has been reasonable, line area (AFP management) will assess what the AFP appointee's duties were at the time, the amount and intent of the usage, and whether the usage distracted the AFP appointee from their primary duties. Professional Standards will only become involved if there is a conduct issue identified and reported as such.

AFP appointees must reimburse the AFP for any usage costs relating to excessive usage which is assessed as beyond reasonable.

The use of social media from mobile devices must be in accordance with the:

- AFP National Guideline on the security of information systems
- Forthcoming Handbook on social media (to be published on the AFP Hub).

15. Private mobile devices used for work purposes (bring your own device or BYOD)

Where approval is given via a security waiver per s. 5 of the AFP National Guideline on the security of ICT hardware and software for the use of an official AFP SIM card to be used in a privately owned mobile device, the use of the device is governed by this guideline. The AFP appointee must be aware of their responsibilities and obligations under this Guideline.

The use of private mobile devices for official business:

- must be authorised in writing by an approver
- is at the AFP appointee's own risk; any damage to, or loss of, a personal mobile device will not, under any circumstances, be covered by the AFP unless authorised as above
- is at the AFP appointee's own expense, which includes bandwidth, software and peripheral costs
- must use the AFP appointee's own device and network support arrangements.

To port a number in or out of the AFP to or from a personal mobile device T&I (see T&I Contact Us page) must be notified by an email from the approver. The approver must ensure all security aspects regarding the transfer have been considered.

AFP appointees must pay any costs associated with breaking their contract .

16. Security

AFP appointees requiring access to secure voice telephony to transmit (secret) classified information for operational reasons must contact Security Reporting and Referrals for advice and assistance.

AFP mobile devices without the approved software installed to manage classified information may only be used to store, process or transmit information up to the level of UNCLASSIFIED.

Mobile devices fully managed by the AFP's device management systems are permitted to store and transmit classified (up to and including PROTECTED) information (this does not include SMS or voice calls). If the mobile device is configured to allow separate sections or containers on the device to increase the personal use functionality, all PROTECTED data must be accessed and stored only through the approved secure applications configured on the mobile device.

Official information and devices must be managed in accordance with the security classification, as per Attachments 1 and 5 to the AFP National Guideline on working in the AFP's classified environments and the AFP National Guideline on information management.

To protect SIM cards from unauthorised use, a SIM PIN must be enabled. If a SIM card has a default PIN, the custodian must change the PIN prior to use.

The AFP reserves the right to audit and remove any misused mobile device or SIM card from AFP appointees without notice.

For further information on National Secure Telecommunication systems refer to the AFP National Guideline on working in the AFP's classified environments and the AFP National Guideline on information management or contact Security Reporting and Referrals.

Malicious cyber activity is a key security risk and therefore all AFP appointees must minimise the contact information stored (particularly on personal or unmanaged mobile devices). On these devices people can inadvertently enable contact information to be automatically and manually backed-up to the Cloud (depending on the mobile device settings). This data is then at risk of unauthorised access.

On these devices AFP appointees must:

- only provide minimal contact details (e.g. a nickname and phone number) and avoid using:
  - full name
  - date of birth
  - AFP references or personal/workplace addresses
- ensure any sensitive numbers (e.g. silent or non-disclosed) or contact details on their device are not backed up to the Cloud
- not add sensitive information (e.g. medical information)
- not add AFP group contact lists.

17. Asset management

Most mobile devices will be allocated as a 'Personal Issue' asset and will need to be sighted periodically for stocktake purposes. When receiving a new mobile device custodians must ensure it is recorded as an asset within their business area in Insight!

AFP appointees issued with an official mobile device are responsible for its safe custody until the asset is transferred. The process for managing the transfer or disposal of assets such as mobile devices is explained in the Asset Management APF Hub page.

When requiring the transfer or deactivation of a carriage service, the custodian must contact T&I (see T&I Contact Us page, http://serviceportal.afp.le/ or call 02 6131 4666, x146666).

When transferring a carriage service to another AFP appointee the custodian must provide the:

- new custodian's details
- new custodian's cost centre
- effective date of transfer.

When AFP appointees resign from the organisation, all mobile devices must be returned as per the AFP National Guideline on separation. Staff will be able to retain their phone number. This can be arranged by contacting T&I (see T&I Contact Us page, http://serviceportal.afp.le/ or call 02 6131 4666, x146666).
Pool mobile devices must be managed by a nominated AFP appointee who must:

- comply with this guideline
- receive the monthly account
- maintain a handover tracking process
- be recorded in Insight! as the custodian and issued with the asset.

Individual users (AFP appointees) of pool mobile devices must:

- comply with this guideline
- identify their personal use on each monthly invoice
- ensure the handover tracking process is followed
- reimburse the AFP for all personal use (see s. 14 above)
- be responsible for the security and appropriate use of the device while in their custody.

18. Loss, theft, damage, or misuse

AFP appointees are responsible and accountable for mobile devices issued to them. Loss or theft of a device could have operational implications.

The process for managing the loss of AFP property such as a mobile device is provided in the AFP National Guideline on loss of relevant money or property.

To avoid possible liability for a lost or stolen mobile device and to protect the AFP data and services contained on the device, the custodian must contact T&I (see T&I Contact Us page or call 02 6131 4666, x146666) during business hours to:

- request the mobile device be deactivated or wiped
- request Mobile Telephone Accounts block the carriage service.

For notification after hours or on public holidays, the custodian must contact the AOCC Supervisor (02 6126 7299) or 131 AFP (131 237).

AFP appointees must also report the loss, theft, damage or misuse of an official mobile device to Security Reporting and Referrals as soon as practicable via a Security Incident Report (AFP Hub) as per the AFP National Guideline on security reporting.

Once the report has been lodged with Security Reporting and Referrals, the custodian must initiate a disposal via Insight!, tick the box saying 'Security Incident Report' and forward a copy of the report to the nominated regional asset controller for final approval. This will allow the mobile device to be removed from the assets register.

19. Further advice

Queries about the content of this guideline should be referred to the Coordinator T&I Assurance and Supplier Management (via TI-Assurance).

20. References

Legislation

- *Australian Federal Police Act 1979* (Cth).

AFP governance instruments

- AFP Commissioner's Order on Professional Standards (CO2)
- AFP Commissioner's Order on Security (CO9)
- AFP National Guideline on loss of relevant money or property
- AFP National Guideline on procurement and contracting
- AFP National Guideline on security reporting
- AFP National Guideline on the security of ICT hardware and software
- AFP National Guideline on the security of ICT system access
- AFP National Guideline on the security of information systems
- AFP National Guideline on the security of removable data storage devices
- AFP National Guideline on separation
- AFP National Guideline on travel and living away from home
- Commissioner's Financial Instructions.
- AFP National Guideline on working in the AFP's classified environments.

Other sources

- AFP Asset Policy (AFP Hub)
- Australian Government Information Security Manual (AFP Hub)
- Australian Government Protective Security Policy Framework (Attorney-General's Department)
- Mobile Device Declaration (AFP Hub)
- Security Incident Report (AFP Hub).
- How to dispose of an asset
- How to transfer assets
- Handbook on social media (forthcoming, to be published on the AFP Hub).