AFP National Guideline on information management

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 this guideline.

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 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
AFPSec	AFP Secret Network
AFPTSN	AFP Top Secret Network
AOCC	AFP Operations Coordination Centre
APP	Australian Privacy Principles
s7(2A)	
CDPP	Commonwealth Director of Public Prosecutions
s37(2)(b)	
s47E(d)	
Cth	Commonwealth of Australia
ICT	Information and communications technology
MOU	Memorandum of understanding
NAA	National Archives of Australia
NAP	Normal administrative practice
PSPF	Protective Security Policy Framework

3. Definitions

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

- engaged overseas under s. 69A of the *Australian Federal Police Act 1979* (Cth) (AFP Act) to perform duties as an AFP employee
- seconded to the AFP under s. 69D of the AFP Act
- engaged under s. 35 of the AFP Act as a consultant or contractor to perform services for the AFP and who has been determined under s. 35(2) of the AFP Act to be an AFP appointee.

(See s. 4 of the AFP Act.)

AFP personnel – includes current and former:

- AFP appointees
- contracted services providers who provide services to the AFP
- AFP volunteers and other personnel who provide services to the AFP.

Disposal authority – is a document that identifies minimum retention periods for Commonwealth records and authorises the destruction of Commonwealth records as required by s. 24 of the *Archives Act 1983* (Cth) and is issued for use across the Commonwealth.

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

Information and communications technology (ICT) – means the technology used to electronically acquire, store, process and distribute information, including telephone and computer systems.

Information management – means managing, in the most efficient way possible, how information is collected, organised, used, controlled, stored, disseminated and disposed of within the AFP.

Information steward – means an AFP appointee, appointed by a manager(s), who is responsible for ensuring the confidentiality, integrity and availability of information in an AFP function or AFP office.

Information system – means a combination of strategic, managerial and operational activities to gather, process, store, distribute and use information and its related technologies.

Manager – means an AFP appointee performing the role of a Senior Executive Service level manager or above.

Metadata – means structured details that are created to describe information resources.

Metadata standard - means an approved set of metadata to describe information resources.

National Manager – means an AFP appointee performing the role of National Manager, Chief Financial Officer, Chief Information Officer or Chief Police Officer for the ACT.

Need-to-know – means a need to access information based on an official AFP requirement and dependent on an appropriate AFP security clearance.

Need-to-share – means that relevant AFP information is available to the right audience in the right context at the right time.

Personal information – means information about an individual whose identity is apparent, or can reasonably be ascertained, from the information.

Police services – is defined in s. 4 of the AFP Act.

Prescribed information – means information obtained by a person in the course of carrying out, performing or exercising any of the person's duties, functions or powers. (See s. 60A of the AFP Act.)

Protective markings – means a visual marking applied to information requiring some form of protection and special handling. s37(2)(b)

s37(2)(b)

Record – means a Commonwealth record as defined in the *Archives Act 1983* (Cth).

Records authority – is a document that identifies minimum retention periods for Commonwealth records and authorises the destruction of Commonwealth records as required by s. 24 of the *Archives Act 1983* (Cth) and is issued for use across the Commonwealth, specific to the functions of the AFP.

Supervisor – means an AFP appointee at or above the position of team leader or rank of sergeant or an AFP contract manager.

System owner – means a senior executive AFP employee responsible for the overall business management, risk acceptance and formal accreditation approval of a designated information system.

System user – means an AFP appointee and other persons appointed, employed, engaged, seconded or otherwise attached to the AFP under the *Australian Federal Police Act 1979* (Cth) or other persons specifically authorised to access AFP information systems.

4. Guideline authority

This guideline was issued by the Deputy Commissioner Close Operations Support 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 outlines the AFP's governance, as well as the obligations for AFP personnel, in relation to information management. The AFP is committed to maintaining trust in, and appropriate control over, all information handled by the AFP.

This guideline should be read in conjunction with the AFP Information Management Policy.

6. Key information management principles

Effective information management processes and practices maximise the efficiencies with which the AFP can receive, create, organise, use, store, disseminate and dispose of information.

Effective information management ensures the integrity of information and enables a single source of truth for information held. A single source of truth means an authoritative, up-to-date source of information is available when required.

AFP personnel must adhere to the need-to-share principle, which is a fundamental premise for the AFP.

System users must only use AFP information systems in a manner ensuring confidentiality and integrity of all information handled by the AFP.

System users should assess and categorise information as soon as possible once it is received or created. This is accomplished largely through the use of metadata. The AFP metadata standard is detailed in Attachment 4.

AFP personnel must comply with all applicable laws and policies in relation to information management.

7. Application

This guideline applies to all system users.

This guideline does not apply to the security of information systems s37(2)(b) s37(2)(b)

8. Information systems

The AFP has various information systems that allow the creation, use, management and dissemination of information. s37(2)(b) s37(2)(b)

9. Receiving information

When information is received from partner agencies, system users must incorporate any caveats on that information into the metadata and record it appropriately as per the AFP Practical Guide on applying security classifications and protective markings to information.

10. Security of information

AFP personnel must protect AFP information from unauthorised use, including release, deletion and modification.

The following information security principles have been adopted:

- **clear desk** – AFP personnel, when absent from the work place, must ensure that security

classified information and other valuable resources are secured appropriately in accordance with the Information and Asset Storage Requirements
- **need-to-know** – AFP personnel must only access information for the purposes of their official duties and at the appropriate level of their security clearance
- **access management** – AFP personnel should recognise the importance of establishing effective access management capability (identity, authentication and authorisation) in relation to information
- **risk management** – AFP personnel must use a risk based approach for assessing threats against information as per the AFP National Guideline on risk management
- **information handling** – AFP personnel must use protective markings to protect and classify information and ensure that classified information is secured appropriately as per the AFP Practical Guide on applying security classifications and protective markings to information.

System users must:

- promote and maintain the security and integrity of all information in AFP information systems
- report any information loss, unauthorised access or unauthorised release via a Security Incident Report (AFP Forms)

s37(2)(b)

10.1 Protective markings

Information in AFP information systems must be given a protective marking in accordance with the AFP Practical Guide on applying security classifications and protective markings to information.

The three types of protective markings are:

- security classifications
- dissemination limiting markers (DLMs)
- caveats.

10.2 AFP Secret Network and AFP Top Secret Network

System users using the AFP Secret Network or AFP Top Secret Network must comply with separate security documentation available on the respective systems. Further information is available on request from Security.

10.3 Communications intelligence material

s37(2)(b), s7(2A)

s37(2)(b), s7(2A)

See the attached Attachment 1 for more details on the security of information.

11. Managing records

AFP personnel must create, capture and manage records to ensure business activity is supported by useable and reliable records. The primary corporate administrative record-keeping system of the AFP is managed via the Records Management module in PROMIS, and records must be kept in a paper format in registry files.

Electronic storage areas such as Outlook, personal or shared drives, or other areas storing electronic information are not record-keeping systems and therefore AFP personnel must not use them as a records management system. These electronic storage areas lack key record-keeping functionality and cannot ensure the integrity and security of the record over time. For example, records in these areas can be:

- deleted
- altered
- inappropriately accessed
- inaccessible when needed.

Information retention

Information retention requirements are subject to the *Archives Act 1983* (Cth) and hard copy files must be created to ensure compliance.

Records are assigned to individuals, teams or organisations in PROMIS and AFP personnel must account for records assigned to them at all times. When records are transferred between individuals the Records Management Unit must be advised so PROMIS can be updated. AFP personnel who are unable to account for their records must submit a Security Incident Report.

Disposal of records

AFP personnel must only destroy records in line with an authorised disposal authority or through the application of normal administrative practice.

See the attached Attachment 2 for more details on managing records.

12. Release of information

When deciding to release or withhold information, AFP personnel must follow the principles of:

- compliance with policies, legislation requirements and directives of the AFP and the Australian Government
- protection of individual interest, third parties and intellectual property rights
- facilitation of AFP, government and community outcomes
- accountability of the individual for releasing information
- need-to-know.

AFP personnel must, when considering any release, note that information release may be lawful

but harmful, unreasonable or inappropriate. AFP personnel, on deciding whether to release information, must consider the relevant circumstances and the range of inter-related and competing interests.

AFP personnel must be aware of the relevant obligations imposed by legislation, the professional standards of the AFP, the expectations of the public, government, other agencies, the AFP Commissioner and colleagues when considering releasing information.

The release of information by consent to an external party or agency requires AFP personnel:

- to hold an authorisation to make a decision to release information, and/or
- to comply with AFP approved procedure or governance relating to particular classes of information (e.g. established procedures to share routine intelligence with a partner agency).

Where there is no specific legislative delegation or authorisation in place, and the request to release information raises integrity, legal or reputational risks for the AFP, a coordinator or above must authorise the release.

12.1 Compulsory release considerations

AFP personnel must consider any lawful compulsion to release information (i.e. subpoena, other court process or legislation) and if the AFP should object to compliance. Requests for advice on objection to release must be referred to AFP Legal, to claim, for example:

- public interest immunity
- legal professional privilege.

If the information sought is owned by, or originates from, a third party, appointees must consult the owner to identify any grounds to refuse release.

Requests to access documents under the *Freedom of Information Act 1982* (Cth) must be handled according to the AFP National Guideline on Freedom of Information releases.

12.2 Accuracy of information

AFP personnel must not release any information which they suspect or know is inaccurate, untrue or misleading, unless authorised to do so by law. Having regard to the intended use of the information, it may be appropriate to:

- verify the accuracy
- provide a disclaimer or caveat as to its accuracy
- provide additional, relevant information.

AFP personnel must submit a Security Incident Report s37(2)(b) s37(2)(b) if they suspect that an unauthorised release has occurred. Any unauthorised release must be investigated by Professional Standards.

12.3 Non-work related release

AFP personnel must not release information for non-official purposes, contrary to:

- s. 60A of the *Australian Federal Police Act 1979* (Cth)
- Division 2.4A of the Australian Federal Police Regulations 1979 (Cth)
- any other legislation or governance instrument.

Where there is a requirement to release information under non-work related circumstances, appointees must both:

- obtain written approval (in any format) from coordinator/superintendent or above prior to information release
- determine on a case-by-case basis, the release of publicly available information (e.g. information available through the Information Publication Scheme on the AFP website).

12.4 Recording information release

AFP personnel who release official information to an external recipient should record the particulars of that release in accordance with AFP governance instruments, legislation and any procedures implemented by respective business areas. Where the information is recorded, the release should be on, or attached to, the document concerned.

See the attached Attachment 3 for more details on the release of information.

13. Removal of information from AFP premises

AFP personnel with a business requirement to remove information protectively marked up to and including CONFIDENTIAL from AFP premises must obtain approval from their supervisor and ensure an audit trail is recorded prior to removing the information.

Information classified Secret or Top Secret or protectively marked with a codeword, must not be removed from AFP premises without written approval from the originating author, business unit or agency. Where approval is obtained, AFP personnel must record and manage the information in accordance with the AFP information handling guides s37(2)(b) s37(2)(b)

AFP personnel must retain the information in their personal custody while removed from AFP premises, unless stored in accordance with the AFP Information and Asset Storage Requirements and the AFP information handling guides (AFP Hub) and the requirements contained within this guideline.

AFP personnel removing information from AFP premises must:

- return and secure it within AFP premises, as per the AFP Information and Asset Storage Requirements, once official offsite work requirements have ceased
- submit a Security Incident Report s37(2)(b) if the information is lost, stolen, released to an unauthorised person(s) or compromised in any way.

Offsite work

The AFP uses the Australian Government Protective Security Policy Framework Working away from the office as a guide to achieving a consistent approach to determining information

security controls when AFP personnel are working away from the office.

For further information on working away from the office, refer to the Offsite Work/Working from Home Hub page.

14. Privacy

AFP personnel must comply with their obligations under the *Privacy Act 1988* (Cth) when obtaining, using and disclosing personal information. The AFP National Guideline on privacy details how to handle personal information.

15. Copyright

System users entering information on AFP information systems grant the AFP the right to edit, copy, republish and distribute such information. If the information has copyright implications, the author should take these into account prior to posting the information on AFP information systems. See also:

- AFP National Guideline on intellectual property, commercialisation, logos and insignia
- AFP National Guideline on software management and copyright.

AFP personnel must consider how copyright obligations (including under s. 183 of the *Copyright Act 1968* (Cth)) affects release, including limiting further usage and marking the information, for example, with '© Commonwealth of Australia 2014'.

16. Responsibilities

All AFP personnel are responsible for managing and controlling AFP information.

National Manager Operations Support is the National Manager responsible for information management in the AFP.

National Managers (and equivalents) must:

- champion AFP information management principles with a focus on their portfolio
- support AFP information management initiatives, maintenance and enhancement of information management infrastructure and the information management processes and practices
- provide direction and guidance on information management issues.

Managers must:

- identify information of value within their functional area, manage it in accordance with this guideline and related governance instruments referenced in this guideline
- promote and ensure awareness of information management responsibilities within their area of responsibility
- appoint information stewards in each function and office to ensure efficient information management practices in their portfolio.

Coordinators and team leaders must:

- ensure their team(s) is aware of role-specific information management responsibilities
- ensure information management activities are aligned with the strategic priorities of the AFP and facilitate efficient and effective services which do not result in duplicated effort
- ensure compliance with the AFP Information Management Policy and this guideline.

All AFP personnel must:

- create and manage information in accordance with this guideline and the referenced governance instruments
- maintain appropriate records of their business activities and decisions
- uphold the confidentiality, integrity and availability of information.

Information stewards

Information stewards are individuals who are the information management champions in their work places. Information stewards must ensure the confidentiality, integrity and availability of the information in their business areas by:

- consulting with system owners and business users to determine business needs
- providing advice to other employees on information management practices
- providing guidance to the managers/National Managers on information management in their business areas
- providing AFP employees with access to adequate training and documentation so they can manage and protect AFP information appropriately.

The information stewards in each AFP function and office are listed on the Information Management Hub page. The information stewards constitute a network and meet with the Information Management Program as required.

17. Further advice

Queries regarding the content of this guideline should be referred to the Information Management Program at Information-Management@afp.gov.au.

18. References

Legislation

- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- *Archives Act 1983* (Cth)
- *Australian Federal Police Act 1979* (Cth)
- *Australian Security Intelligence Organisation Act 1979* (Cth)
- *Crimes Act 1900* (ACT)
- *Crimes Act 1914* (Cth)
- *Crimes (Child Sex Offenders) Act 2005* (ACT)
- *Crimes (Controlled Operations) Act 2008* (ACT)
- *Financial Transaction Reports Act 1988* (Cth)
- *Freedom of Information Act 1982* (Cth)
- *Intelligence Services Act 2001* (Cth)
- *Law Enforcement Integrity Commissioner Act 2006* (Cth)
- *Mutual Assistance in Criminal Matters Act 1987* (Cth)

- *Parliamentary Joint Committee on Law Enforcement Act 2010* (Cth)
- *Privacy Act 1988* (Cth)
- *Proceeds of Crime Act 2002* (Cth)
- *Public Interest Disclosure Act 2013* (Cth)
- *Safety, Rehabilitation and Compensation Act 1988* (Cth)
- *Telecommunications Act 1997* (Cth)
- *Telecommunications (Interception and Access) Act 1979* (Cth)
- *Witness Protection Act 1994* (Cth).

AFP governance instruments

- AFP Commissioner's Order on Professional Standards (CO2)
- AFP National Guideline on controlled operations under Commonwealth law
- AFP National Guideline on external agreements
- AFP National Guideline on Freedom of Information releases
- AFP National Guideline on intellectual property, commercialisation, logos and insignia
- AFP National Guideline on international police-to-police assistance in death penalty situations
- AFP National Guideline on offshore situations involving potential torture or cruel, inhuman or degrading treatment or punishment
- AFP National Guideline on privacy
- AFP National Guideline on public interest disclosure
- AFP National Guideline on risk management
- s37(2)(b)
- AFP National Guideline on software management and copyright

s37(2)(b)

- AFP Practical Guide on conducting controlled operations under ACT law
- AFP Practical Guide on Requesting Legal Advice from AFP Legal

s37(2)(b)

- Information Management Policy.

Other sources

- Australian Government Protective Security Policy Framework.

19. Attachments

Attachment 1 – Security of information

The Australian Government Protective Security Policy Framework (PSPF) outlines how the Australian Government takes appropriate measures to protect its people, information and assets, at home and overseas.

Overlooking and overhearing

System users must ensure that unauthorised persons cannot see information displayed on computer screens. Particular care must be taken with higher classified systems such as AFPSec and the AFPTSN.

AFP appointees must consider who can, or may, overhear a conversation, including conversations of other persons (i.e. not just conversations the AFP appointee is directly involved in).

AFP appointees must not discuss AFP information or that which may bring the AFP into disrepute or compromise third party information, in any public place/facility or any non-approved government facility.

AFP appointees must only use desktop (voice over internet protocol) telephones for conversations up to and including PROTECTED where the other party is internal to AFP premises.

AFP appointees must only use desktop telephones and cordless telephones using the public telephone network, mobile telephones and the teleconferencing system for UNCLASSIFED conversations. Where conversations of 'For Official Use Only' or above are required over teleconferencing systems, contact Security for advice.

s37(2)(b)

For further information on National Secure Telecommunication systems refer to the s37(2)(b) s37(2)(b)

Storage

Hard copy information must be secured when not in use to prevent access by unauthorised persons. Access to information marked PROTECTED or above must be strictly controlled and remain in the close personal custody of the AFP appointee.

The level of physical security required will depend on the business impact level of any compromise, loss of confidentiality, integrity or availability of information, or the potential for harm to AFP appointees or members of the public. All controls identified in the PSPF – Australian Government physical security management guidelines—Security zones and risk mitigation control measures must be considered.

Transport

AFP appointees must take protective measures when transporting information outside of AFP premises. This can include approved briefcases, satchels, seals, pouches or transit bags. Refer to the PSPF – Australian Government information security management guidelines—Protectively marking and handling sensitive and security classified information.

Information and security briefcases or containers must not be exposed to casual observation or left unattended. When traveling by air, information must be treated as carry-on baggage.

Attachment 2 – Records management

AFP Records Management must ensure records are:

- managed in accordance with legislation

adequately registered and classified in a record-keeping system, regardless of format
- managed to comply with the Australian Government Protective Security Policy Framework (PSPF)
- appropriately and accurately sentenced, and disposed of, in accordance with a disposal authority issued by the National Archives of Australia.

Retention and disposal

Records must be retained for the period, and in the manner, set down by relevant legislation, regulations, guidelines and disposal authority schedules issued by the National Archives of Australia.

Records must not be destroyed unless the destruction is:

- authorised by an appropriate disposal authority, issued by the National Archives of Australia, or by the provisions of relevant legislation
- approved by the original owner of the record(s)
- performed on an exact duplicate of the original used only for reference.

The only area permitted to destroy official AFP records is the AFP Records Management Unit. Records of the destruction must be retained permanently as national archives.

Destroying records must:

- comply with the PSPF – Australian Government information security management guidelines—Protectively marking and handling sensitive and security classified information
- be secure and environmentally sound
- comply with legislation and guidelines, including those of the National Archives of Australia.

Destruction as normal administrative practice

The AFP normally requires authorisation from the National Archives of Australia to lawfully dispose of official AFP information. However, s. 24 of the *Archives Act 1983* (Cth) allows for disposal without this authority where normal administrative practice (NAP) applies to disposing of records containing no obviously valuable information.

The NAP provision must not replace the records disposal arrangements agreed to in disposal authorities.

Appointees in doubt about whether NAP applies must put the document in a record-keeping system or contact AFP Records Management for advice.

To decide if records can be disposed of through NAP, appointees must consider whether unique and valuable information would be lost (e.g. a telephone message from a minister containing information important to AFP business must be kept if it is not recorded elsewhere).

NAP usually allows the following Commonwealth records to be disposed of:

- superseded manuals or instructions (except for a master set which includes the superseded portions)
- library material (except for assets to be ‘written-off’)
- catalogues and trade journals

- information copies of press cuttings, press statements or publicity material
- letters of appreciation or sympathy
- requests for copies of maps, plans, charts, advertising material or other stock information
- address lists and change of address notices
- calendars, office diaries and appointment books (unless identified in records disposal authorities as having additional value)
- facsimiles, where a photocopy has been made for file
- rough drafts of reports, correspondence, or routine or rough calculations
- draft documents produced for internal (within the team) consultation which do not contain significant changes of direction or alteration of the intent of the document
- routine statistical and progress reports compiled and duplicated in other reports
- abstracts or copies of formal financial records maintained for convenient reference
- telephone messages, when the fact of the call or the content of the call is not relevant to AFP business
- 'With Compliments' slips
- non-acceptance of invitations
- trivial electronic mail messages or notes not related to agency business
- out-of-date distribution lists.

When normal administrative practice must not be used

AFP personnel must not use NAP for:

- disposing records that detail significant operations which may have a long-term value
- allowing the destruction of records which document the rights and obligations of the government or private individuals
- culling papers from files (NB: papers should only be culled according to a specific disposal authority)
- disposing business related email before it becomes part of the formal record
- disposing policy documents
- disposing significant drafts of documents which provide evidence of changes in direction or AFP-wide comment
- audio and video tapes of records of interview
- accountable diaries, field books and notebooks
- charge sheets and charge books.

NAP may also be restricted or revoked for records subject to a disposal freeze imposed by the National Archives of Australia.

Where NAP is not permitted as described above, advice should be sought on the appropriate course of action from the RMU National Help Desk.

Queries regarding managing records should be referred to AFP Records Management s47E(d) s47E(d)

Attachment 3 – Release of information

Release of information is a fundamental part of the AFP's law enforcement role and responsibilities. AFP personnel may be required to release AFP information outside the organisation at various times.

Information release situations

Although the obligations set out in this Attachment can apply to all releases of information, the following are examples where AFP personnel may need to make decisions about information release:

- requests from members of the public, including from individuals and organisations
- requests from the media
- AFP media releases
- requests from government, including questions on notice and ministerial inquiries
- requests to assist Australian and foreign law enforcement agencies
- disclosure of evidence to courts and tribunals
- dissemination of intelligence products
- responses to compulsory production notices such as subpoenas, or requests under the *Freedom of Information Act 1982* (Cth) or the *Privacy Act 1988* (Cth) release for professional or research purposes.

The range of scenarios in which information release may occur is very broad. Care must be taken to examine the purpose of the release and the nature of the information proposed to be released.

In relation to higher risk requests to release information involving integrity, legal and reputational risks, AFP personnel must obtain the approval of a coordinator or above to authorise the release.

Any queries regarding the effect of legislation on the release of information should, in the first instance, be directed to a supervisor. If necessary, queries may be directed to AFP Legal for clarification in accordance with the AFP Practical Guide on Requesting Legal Advice from AFP Legal.

Key legislative requirements

Legislative requirements, particularly the *Australian Federal Police Act 1979* (Cth) (AFP Act) and *Privacy Act 1988* (Cth), are the primary rules which govern information release by AFP personnel.

Australian Federal Police Act 1979

Section 60A of the AFP Act is the primary prohibition against, and authority for, AFP appointees to release and record information obtained by them in the course of carrying out, performing or exercising any of their duties, functions or powers under the AFP Act.

Section 60A permits AFP appointees to release or make a record of **prescribed information** only for the purposes of carrying out, performance or exercise of any of the person's duties, functions or powers under the AFP Act, the *Witness Protection Act 1994* (Cth), the *Law Enforcement Integrity Commissioner Act 2006* (Cth), the *Parliamentary Joint Committee on Law Enforcement Act 2010* (Cth) and their regulations.

Duties are defined to include responsibilities. Powers is defined to include authorities, rights privileges and immunities. The AFP functions are those outlined in s. 8 of the AFP Act. Those functions are:

- to provide police services and police support services in relation to:
    - the Australian Capital Territory
    - the Jervis Bay Territory and certain other Commonwealth Territories
    - the laws and property of the Commonwealth and the safeguarding of Commonwealth interests
    - assisting, or cooperating with, Australian or foreign:
        - law enforcement
        - intelligence
        - security
        - government regulatory agencies
    - establishing, developing and monitoring peace, stability and security in foreign countries
- investigating state offences with a federal aspect
- functions conferred by:
    - the *Witness Protection Act 1994* (Cth)
    - the *Proceeds of Crime Act 2002* (Cth)
- performing such protective and custodial service functions as the Minister directs by notice in writing in the Gazette
- doing anything incidental or conducive to the performance of the above functions.

Compliance with s. 60A often requires careful examination of the above list to ensure that the release is consistent with the AFP appointee's duties, functions or powers.

Release of information contrary to s. 60A of the AFP Act is a criminal offence carrying a maximum penalty of two years imprisonment. Other key legislative provisions include, in the Australian Federal Police Regulations 1979 (Cth):

- r. 13B in relation to unauthorised disclosure of information relating to professional standards matters under Part V of the AFP Act
- r. 13C in relation to unauthorised use of access to information by reason of being an AFP appointee.

Privacy Act 1988

AFP personnel must comply with the *Privacy Act 1988* (Cth). The Australian Privacy Principles (APP) in the schedule to the Privacy Act governs the handling of personal information. APP 6 governs the use and release of personal information in Australia. APP 8 governs the release of personal information overseas.

APP 6.2 sets out the circumstances in which the use or release of information about an individual is permitted. These include:

- use or release by a law enforcement body where it is necessary for a law enforcement related activity
- where use or release of personal information is required or authorised under an Australian law.

For more information refer to the AFP National Guideline on privacy.

Other important legislative restrictions

Legislation may either restrict the release of information or authorise it subject to limitations. Restrictions upon the release of information exist in over 150 pieces of legislation. These restrictions include:

Crimes Act 1914

Section 70 of the Act provides non-disclosure provisions for a person who is or was a Commonwealth officer. For more information, refer to the Aide Memoire on unauthorised disclosure of information by Commonwealth employees.

Additionally, the *Crimes Act 1914* (Cth) contains numerous provisions regarding the use and disclosure of various types of information.

Public Interest Disclosure Act 2013

Section 65 provides that protected information may only be used and disclosed for permitted purposes. For more information, refer to the AFP National Guideline on public interest disclosure.

Search Warrants

Commonwealth

Material seized pursuant to a search warrant obtained under s. 3E of the *Crimes Act 1914* (Cth) can only be shared or disclosed for certain purposes in accordance with s. 3ZQU of that Act. More details about the permitted use of seized material can be found in the Commonwealth Director of Public Prosecutions Search Warrant Manual and in the Investigator's Toolkit.

ACT Policing

Under s. 195(5) of the *Crimes Act 1900* (ACT), things seized under a search warrant may be made available to officers of other agencies if it is necessary to do so for the purpose of investigating or prosecuting an offence to which the things relate.

The AFP may share objects with state and territory law enforcement agencies under extra-territorial search warrant arrangements under s. 258 of the *Crimes Act 1900* (ACT).

For more information, refer to the Australian Capital Territory specifics in the Investigator's Toolkit.

Biometric data stored on law enforcement databases

The AFP collects, records and discloses biometric data which is stored on a range of shared information databases hosted by CrimTrac. These databases include DNA, fingerprint and facial recognition information. The *Crimes Act 1914* (Cth) contains provisions about the use and disclosure of biometric data.

s37(2)(b)

Registered child sex offender information

Commonwealth

The AFP has limited access to the Australian National Child Sex Offender Register (ANCOR) for the purpose of prevention of child sex offences. s37(2)(b)

s37(2)(b)

ACT Policing

Within the ACT, child sex offenders are registered and monitored under the *Crimes (Child Sex Offenders) Act 2005* (ACT). This Act places strict limitations on the use and disclosure of information relating to registered offenders. For more information, refer to the Aide Memoire on ACT Policing Child Sex Offenders Registry Team.

Telecommunications interception product

Disclosure of lawfully intercepted information or warrant information is prohibited under s. 63 of the *Telecommunications (Interception and Access) Act 1979* (Cth). There are some exceptions where authorised under the Act or for a permitted purpose. Further information in relation to use and disclosure of telecommunication interception product can be found in the CDPP Telecommunications Interception and Stored Communications Warrant Manual.

Telecommunications data

Disclosure of telecommunications data is governed by Division 6 in Part 4-1 of the *Telecommunications (Interception and Access) Act 1979* (Cth). s37(2)(b)

s37(2)(b)

Financial information

Restrictions on the release of certain financial information is governed by the:

- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- *Financial Transaction Reports Act 1988* (Cth).

There are exceptions allowing use and release in certain circumstances.

Intelligence agency information

Specific restrictions apply to the disclosure of information from the intelligence community in certain situations. Section 18 of the *Australian Security Intelligence Organisation Act 1979* (Cth) and Part 6 the *Intelligence Services Act 2001* (Cth) contain offences for disclosure of intelligence information without authorisation.

Surveillance device product

Disclosure of protected information is restricted by s. 45 of the *Surveillance Devices Act 2004* (Cth). This section also provides for circumstance where disclosure is permitted. More details about the permitted use of seized material can be found in the Commonwealth Director of Public Prosecutions Surveillance Devices Manual.

Controlled operations

Commonwealth

Commonwealth controlled operations are governed by Part IAB of the *Crimes Act 1914* (Cth), which also contains offences for disclosing information about controlled operations. Further information is contained in the Investigator's Toolkit s37(2)(b) and the AFP National Guideline on controlled operations under Commonwealth law.

ACT Policing

Unauthorised disclosure of information concerning ACT controlled operations is governed by s. 26 of the *Crimes (Controlled Operations) Act 2008* (ACT). For more information, refer to the AFP Practical Guide on conducting controlled operations under ACT law.

Witness protection

The protection of witnesses relies heavily on the confidentiality of information. Disclosure of information in relation to the National Witness Protection Program (NWPP) is restricted by the *Witness Protection Act 1994* (Cth).

s37(2)(b)

s37(2)(b)

Freedom of Information Act 1982

Any person may forward a written request for documents under the *Freedom of Information Act 1982* (Cth) (FOI Act) to the AFP. The AFP Hub provides a link to the Information Access Team page which provides more detail on this matter.

Under the FOI Act, the AFP is also required to publish non-exempt 'operational' information on the AFP's external website under the Information Publication Scheme (IPS). This includes publishing operational information, as defined by the FOI Act, about the AFP's functions or powers in making decisions that affect members of the public. Only documents approved for publication are published on the IPS.

Statutory compulsory production

Commonwealth and state agencies may have powers under legislation to serve a notice on the AFP to produce information. The AFP is compelled to comply with any statutory production notices in the same way as a subpoena. An example is a s. 71 notice under the *Safety, Rehabilitation and Compensation Act 1988* (Cth) issued by Comcare to produce documents or information.

Release of information for court purposes

Subpoenas

Responding to subpoenas is a normal part of the AFP's responsibilities as a law enforcement agency. The Aide Memoire on subpoenas contains further information for responding to a subpoena, which is generally applicable to other types of proceedings.

Appearing as a witness in legal proceedings

As a witness in legal proceedings, AFP personnel may be allowed to claim some of the exceptions against disclosing information set out in this attachment. The principles of making claims for privilege exempting material from being introduced into oral evidence are the same as for those exempting written evidence for production to a court. If AFP personnel are a witness in a proceeding where they believe they may need to claim privilege against giving oral evidence on a matter, they should contact AFP Legal at the first available opportunity to discuss their concern.

Prosecution disclosure obligations

Prosecution disclosure is an obligation upon the prosecution to inform the defendant of:

- the prosecution's case against them
- any information in relation to the credibility or reliability of the prosecution witnesses
- any unused material.

AFP case officers have a duty to provide the Commonwealth Director of Public Prosecutions (CDPP), ACT Director of Public Prosecutions or state/territory prosecuting authority with relevant information to satisfy these obligations.

Privileges and immunities

Legal professional privilege

Legal professional privilege is an important protection against the disclosure of communications between a lawyer and client. It also applies to communications with AFP Legal and the CDPP. Further information is available in the Investigator's Toolkit.

Public interest immunity

Public interest immunity is immunity from the disclosure of information, including production under a subpoena, which recognises that the release of some information would be contrary to the public interest if it was to be revealed in proceedings. s37(2)(b)

s37(2)(b)

Memorandums of understanding and AFP governance

Domestic and international agreements

The AFP is a signatory to many domestic and international external agreements and memorandums of understanding (MOUs) where information sharing arrangements are agreed between parties. While they are not legally binding documents, MOUs provide guidance on agreed processes for information sharing and should be consulted where a relevant disclosure is being considered.

Specific documents provided by law enforcement or intelligence agencies may include caveats on use and disclosure. AFP personnel need to carefully read caveats in regard to the use, disclosure or disposal of documents provided by third parties.

Under an external agreement framework, AFP appointees may be appointed state/territory special constables or have access to the statutory powers of officers of other Commonwealth or

state agencies. In these situations, AFP appointees must familiarise themselves with obligations to comply with applicable legislation and agency governance obligations upon information management and disclosure. AFP appointees should seek advice from their supervisor and/or from external agencies if they require guidance in relation to handling external agency information.

AFP appointees may also have direct access to databases provided by state and territory police services and other agencies. AFP appointees must comply with an external agreement and the applicable legislation and database terms and conditions applying to access, use and release of information.

For more information refer to the AFP National Guideline on external agreements.

Death penalty

The AFP National Guideline on international police-to-police assistance in death penalty situations provides guidance on considerations for disclosure of information in such situations, together with guidance on the approval process that must be followed.

Torture or cruel, inhuman or degrading treatment or punishment

The AFP National Guideline on offshore situations involving potential torture or cruel, inhuman or degrading treatment or punishment provides guidance on issues to consider and approval processes that must be followed in such situations.

Mutual assistance requests

All mutual assistance requests made by the AFP are coordinated through the AOCC. Information provided by the Commonwealth Attorney-General's Department about what information should be included in a mutual assistance request is available on the Hub.

Generally, information obtained from foreign jurisdictions pursuant to a mutual assistance request can only be used for that investigation. See s. 43B of the *Mutual Assistance in Criminal Matters Act 1987* (Cth).

Release for professional or research purposes

AFP personnel may release information in a private capacity, where approved, for professional or research purposes where it either:

- coincides with an authorised AFP law enforcement purpose
- is consistent with relevant legislation and this guideline.

Professional or research purposes may include, but are not limited to:

- public lectures and speeches
- professional associations or societies
- responses to questionnaires or surveys
- communications and/or interviews with the media
- film, radio and television appearances
- statements to non-government bodies
- books, articles, letters or other textual material, whether purporting to be fact or fiction
- participation in outside study conferences, seminars, symposiums and discussions
- theses for academic studies.

A request by AFP personnel to use or release information for a professional or research purpose is subject to the **same** considerations as a request by a member of the public to use or access that information.

AFP personnel must, in the first instance, submit a written application to their manager or National Manager and Corporate Communications if they wish to engage in any public (including academic) activity which may involve either:

- release of information and/or experience obtained in the course of official duties
- public expression of views on official matters.

The application, which must be in writing (in any format), must:

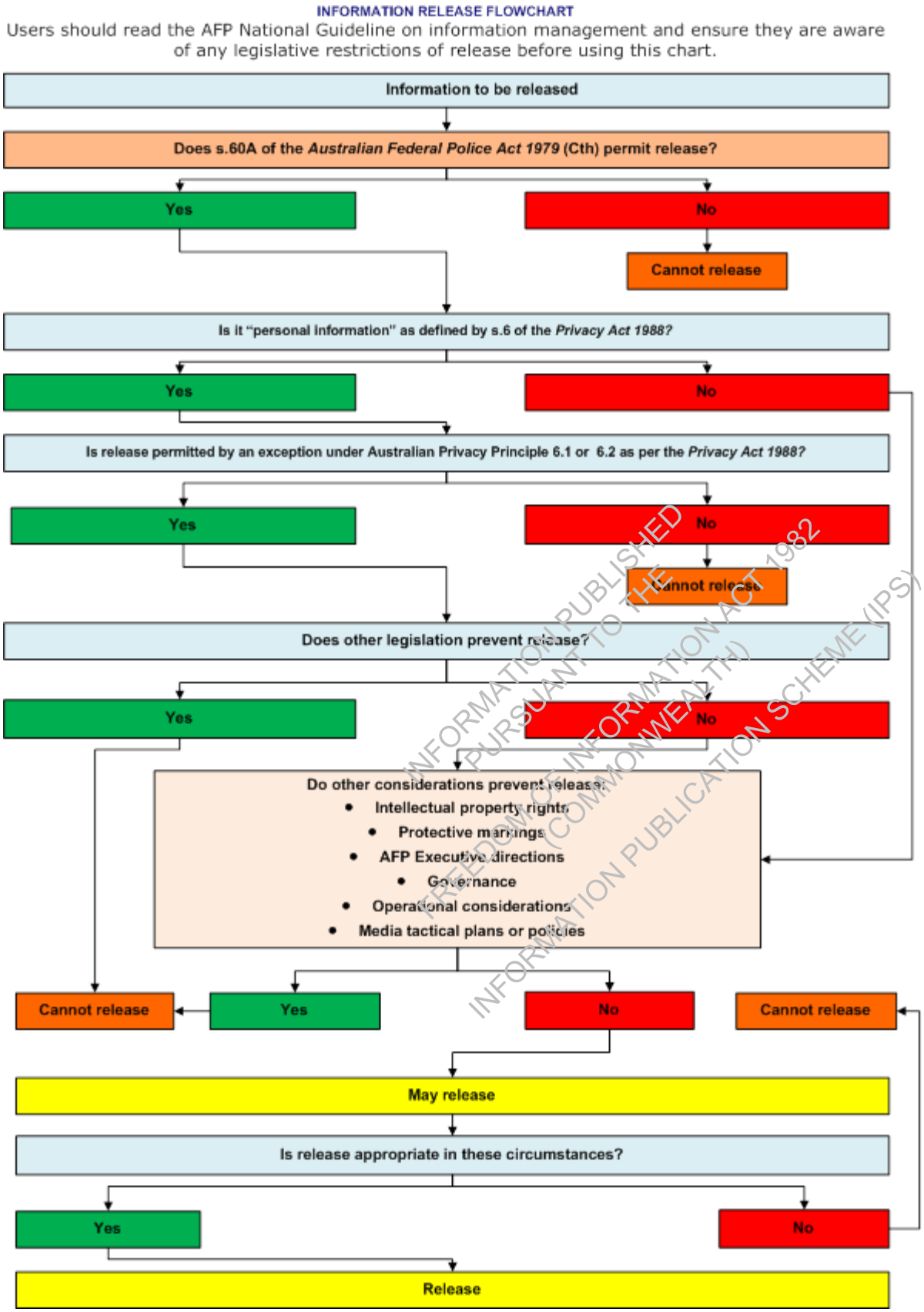
- clearly articulate any likely benefit to the AFP
- consider the risk management surrounding the use or disclosure of official information, in accordance with the AFP National Guideline on risk management
- be submitted with sufficient time to allow proper consideration of the request
- be forwarded to the relevant manager or National Manager.

Functional information owners must only approve the release of information (including to members of the public) if they consider it is both lawful and appropriate to do so, in accordance with this guideline.

Applications by AFP personnel should be returned to the person via their manager, whether approved or not. If approved, the person's manager must ensure the person is aware of their release responsibilities **prior** to any public release or use of information, including:

- non-release of security classified information (sanitise where necessary)
- non-release of any hard copy material, unless specifically authorised and protectively marked 'UNCLASSIFIED'
- awareness that remarks may be reported and/or considered as official AFP opinion. Discernment must be exercised when making any public comment or statement.
- release must be limited to what has been approved and:
    - must not conflict with the interests of the AFP or government policy
    - must not bring the AFP into disrepute or compromise third party information
    - may be done to clarify matters of **fact** where silence may be interpreted as agreement or support
    - may include, in non-committal and professional terms, possible alternative policies, procedures or courses of action and the perceived advantages or disadvantages

associated with them.



Attachment 4 – Metadata standard

The below minimum metadata standard has been endorsed by the AFP. System users must

ensure this metadata is applied to all information resources created and uploaded into all AFP information systems where the information system allows. AFP information systems will either automatically generate metadata or prompt the user to select the metadata.

Element	Definition
Creator	The entity primarily responsible for creating/uploading the resource.
Date	The date the resource is uploaded.
Function	The topic of the resource as defined by the National Archives of Australia (NAA).
Activity	The nature of the content of the resource as defined by the NAA.
Identifier	An unambiguous reference to the resource within a given context.
Protective marking	The security classification of the resource.
Publisher	The entity primarily responsible for making the resource available. Also the owner of the resource.
Title	The name given to the resource.

Information systems

System owners must ensure that information systems incorporate the metadata standard above as soon as practical where the system allows.