AFP National Guideline on privacy

1. Disclosure and compliance

- This document is classified **OFFICIAL** and is intended for internal AFP use.
- Disclosing any content must comply with Commonwealth law and the AFP National Guideline on information management.
- This instrument forms part of the AFP Governance Instrument Framework (GIF) as defined in the AFP Commissioner's Order on governance (CO1). The AFP Commissioner's Order on professional standards (CO2) and AFP Commissioner's Order on security (CO9) set the framework for the conduct expected of AFP appointees through obligations and best practice to help maintain the safety and security of AFP information, operations, assets and people. Inappropriate departures from the provisions outlined within AFP governance instruments may constitute a breach and be dealt with under Part V of the *Australian Federal Police Act 1979* (Cth)

2. Guideline authority

- This guideline was issued by Chief Counsel using power under s. 37(1) of the *Australian Federal Police Act 1979* (Cth) as delegated by the Commissioner under s. 69C of the AFP Act.

3. Introduction

- This guideline outlines the obligations of AFP appointees arising from the Australian Privacy Principles (APPs), the role of the AFP's Privacy Champion and Privacy Officers, and how the AFP manages privacy complaints. This guideline helps control Enterprise Risk 8: Information, so that the AFP is able to effectively operate, and retain the trust of AFP appointees, the Government, community and its partners.
- In addition to the obligations prescribed in the APPs, AFP appointees must ensure all information that is collected, used, shared, accessed after collection, stored and transmitted in many forms including electrical, physical and verbal meets the minimum handling requirements as established within the broader Protective Security Policy Framework (PSPF) policies. Information management specific PSPF policies include, but are not limited to:
- Part 3 (Information), Policy 9 (Classification and Caveats)
- Part 3 (Information), Policy 10 (Information Holdings)
- Part 3 (Information), Policy 11 (Information Disposal)
- Part 3 (Information) Policy 12 (Information Sharing)

4. Australian Privacy Principles

- The APPs are located in Schedule 1 of the *Privacy Act 1988* (Cth) (Privacy Act) and are summarised in s.6 of this guideline. Each APP imposes specific obligations on the AFP and governs the way the AFP collects, uses, discloses and stores personal information. Under s. 15 of the Privacy Act, the AFP **must not** act in any way that breaches an APP.
- AFP appointees should also refer to the Australian Privacy Principles guidelines and the Australian Privacy Principles quick reference tool (both published by the Office of the Australian Information Commissioner (OAIC) and available at www.oaic.gov.au) for more detailed information about their APP compliance obligations.

5. Personal information

- ***Personal information*** means information or an opinion about an identified individual (or an individual who is reasonably identifiable) regardless of whether the information or opinion is:
- true (or not)
- recorded in a material form (or not).
- Examples of personal information include a name, address, or date of birth. Information obtained from open sources such as social media may also contain personal information (e.g. an individual's Facebook profile picture). Personal information that is collected by the AFP can often include sensitive information. **Sensitive information** means information or an opinion about an individual's:
- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual preferences or practices
- criminal record
- health or genetic information
- biometrics (as used for automated biometric verification or identification, including templates).
- AFP appointees must take particular care when collecting, using or disclosing sensitive information as this information is generally afforded a higher level of privacy protection under the APPs than other personal information.
- Information about deceased persons is not personal information and is therefore not covered by the Privacy Act; however, the AFP should endeavour to respect the sensitivities of family members when using or disclosing this information.
- PSPF Policy 8 mandates that 'personal to sensitive' information about an individual must have the appropriate security classification marker assigned to the information. The originator of the information assigns the 'sensitive to security classified marker' and remains responsible for the control of the sanitisation, reclassification or declassification of information. 'Official: Sensitive' is the baseline marker for 'personal to sensitive' information. Aggregated or integrated information may require a higher security classification marker than 'Official: Sensitive' (refer to Part 3 (Information), Policy 10 (Information Holdings)).
- If the originator of the information approves the reclassification or declassification of information, they must record the change in accordance with PSPF Policy 8 section C.2.6.36.

6. Specific obligations

- The APPs set out standards, rights and obligations around the handling of personal information by entities, including the AFP.
- These are set out in detail at Attachments 1-5 and include:

APP 1 – Open and transparent management of personal information

- Requires the AFP to have a Privacy Policy that may be accessed by the public, and practices and procedures to ensure compliance with the APPs and any registered APP code that binds the AFP, including the Privacy (Australian Government Agencies — Governance) APP Code 2017 (Cth) (Privacy Code).

APP 2 – Anonymity and pseudonymity

- Requires the AFP to give individuals the option of remaining anonymous or using a pseudonym when dealing with the AFP unless:
- it is impractical to deal with an individual in this way
- the AFP is required or authorised by an Australian law or an order of a court/tribunal to deal with individuals who have identified themselves.
- AFP appointees should refer to Attachment 1 for more details on APP 2 and their obligations under it.

APP 3 – Collection of solicited personal information

- Details when the AFP can collect personal information that is required or requested (solicited) from individuals, and applies higher standards to the collection of sensitive information.

Personal information

- The AFP should only collect personal information when it is 'reasonably necessary' for, or is directly related to, the AFP's functions.
- 'Reasonably necessary' is an objective test. The following factors may be important in determining whether collection is reasonable:
- the primary purpose of collection
- how the information will be used
- whether the activity could be undertaken without collecting the information.
- Personal information should be collected directly from the individual unless one of the following applies:
- the individual consents to the collection of personal information from a third party
- the AFP is required or authorised by an Australian law or a court/tribunal to collect the information from someone other than the individual
- it is unreasonable or impracticable to do so.

Sensitive information

- Sensitive information should only be collected when it is reasonably necessary for, or is directly related to, one or more of the AFP's functions and the individual consents to the collection.
- There are a number of exemptions that enable the AFP to collect sensitive information without the consent of the individual whose information is being collected. The most relevant of these are:
- when the information is required or authorised by an Australian law or an order of a court/tribunal

- where the AFP, as an enforcement body, reasonably believes the collection of the information is reasonably necessary for, or directly related to, one or more of the functions of the AFP.
- AFP appointees should refer to Attachment 2 for more details on APP 3 and their obligations under it.
- **APP 4 – Dealing with unsolicited personal information**
- Details how the AFP must deal with the collection of personal information and sensitive information that is not required or requested (unsolicited) from individuals.
- **APP 5 – Notification of the collection of personal information**
- Details when and what the AFP must tell an individual about the collection of their personal information.
- APP 5 lists a number of matters that should be notified; however, generally the individual should be made aware of how and why their personal information is or will be collected, and what the AFP will do with the information. The notification should occur at or before the time of collection, or if that is not practical, as soon as possible after the collection.
- AFP appointees must assess, on a case-by-case basis, whether it is reasonable to notify an individual of the collection of their personal information (noting that it may be reasonable to not notify an individual or person of interest subject to an investigation or other police inquiry).
- AFP appointees should refer to Attachment 3 for more details on APP 5 and their obligations under it.
- **APP 6 – Use or disclosure of personal information**
- Details the circumstances in which the AFP may use or disclose the personal information it holds. Generally, personal information must not be used or disclosed for a purpose other than the primary purpose for which it was collected, unless either:
- the individual concerned has consented to its release for that secondary purpose
- a specific exemption applies.
- There are a few exemptions that enable AFP appointees to use or disclose personal information without consent, including when it is either:
- reasonably necessary for one or more enforcement related activities conducted by the AFP (or on behalf of an enforcement agency)
- required or authorised by an Australian law or an order of a court/tribunal.
- AFP appointees must:
- assess, on a case-by-case basis, each use or disclosure of personal information to determine if it is required
- determine if the disclosure is consistent with the functions of the AFP.
- Where the disclosure or use is consistent with the above, an exemption may apply to permit the use or disclosure. Note: the disclosure of personal information overseas is governed by APP 8. AFP appointees should refer to Attachment 4 for more details on APP 6 and their obligations under it.
- **APP 7– Direct marketing**

- Details the conditions that must be met for an organisation to use or disclose personal information for direct marketing purposes. Direct marketing involves communicating directly with a consumer to promote the sale of goods and services. It does not apply to the AFP.
- **APP 8 – Cross-border disclosure of personal information** Details the steps the AFP must take to protect personal information before it is disclosed overseas. AFP personnel disclosing personal information overseas must take reasonable steps in the circumstances to ensure the overseas recipient does not breach the APPs.
- Overseas disclosure of information does not include providing personal information on AFP systems to AFP appointees working overseas (this is a 'use' of information and is governed by APP 6).
- There are a number of possible exemptions that permit the disclosure of personal information overseas, including if the disclosure:
- is required or authorised by an Australian law or an order of a court/tribunal
- of the information is reasonably necessary for one or more enforcement related activities conducted by an enforcement body (such as the AFP) and the recipient is a body that performs functions or exercises powers similar to those exercised by an enforcement body.
- If the disclosure is consistent with the functions of the AFP, then an exemption may apply. AFP appointees must assess each disclosure on a case-by-case basis and also consider whether either of the following applies:
- 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 appointees should refer to Attachment 5 for more details on APP 8 and their obligations under it.
- **APP 9 – Adoption, use or disclosure of government related identifiers**
- Details the limited circumstances when an organisation may adopt, use or disclose a government-related identifier. It does not apply to the AFP.
- **APP 10 – Quality of personal information**
- Requires the AFP to take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete. The AFP must also take reasonable steps, having regard to the purpose of the use or disclosure, to ensure personal information it uses or discloses is accurate, up-to-date, complete and relevant. There may be circumstances when it may not be reasonable to update information, such as when that information would be useful to maintain in its preserved form.
- AFP appointees should refer to the AFP National Guideline on information management for their obligations in relation to capturing, storing, maintaining and managing full and accurate records.
- **APP 11 – Security of personal information**
- Requires the AFP to take reasonable steps to protect the personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. The AFP also has obligations to destroy or de-identify personal information in certain circumstances.
- AFP appointees should refer to the AFP National Guideline on information management and the AFP National Guideline on information security for their obligations in relation to securing information.

- **APP 12 – Access to personal information**
- Details the AFP's obligations when an individual requests access to their personal information. This is a separate access regime from the *Freedom of Information Act 1982* (Cth) (FOI Act) (See the AFP National Guideline on Freedom of Information releases.)
- AFP appointees must refer to any requests from members of the public for access to personal information to the Freedom of Information Team in AFP Legal.
- **APP 13 – Correction of personal information**
- Details the AFP's obligations in relation to correcting the personal information held about individuals. There is also a regime to correct information under the *FOI Act*.
- The principle requires the AFP to take reasonable steps to correct personal information if the AFP considers the information to be inaccurate, out-of-date, incomplete, irrelevant or misleading.
- If the AFP corrects the individual's personal information, the individual may also ask the AFP to notify any entity to which it had previously disclosed the information of that correction. If this occurs, reasonable steps must be taken to notify the entity. Such notification is not required if it would be impracticable or unlawful.
- AFP appointees must refer requests to correct personal information to the Freedom of Information Team in AFP Legal.

7. Privacy Management Plan

- The Privacy Code requires the AFP to develop a Privacy Management Plan (PMP) which identifies specific, measurable privacy goals and targets and sets out how the AFP will meet its compliance obligations under APP 1.2.
- The Privacy Officer manages the AFP's performance under the PMP.

8. Privacy Officer

- The designated Privacy Officer sits within AFP Legal and is a member of the OAIC's Information Contact Officers Network. The Privacy Officer may be one or more persons within AFP Legal designated to undertake this function.
- The functions of the Privacy Officer under the Privacy Code and other OAIC governance include:
- advising AFP appointees about privacy issues
- maintaining a record of the AFP's personal information holdings
- recording and reporting on privacy issues and breaches
- responding to external queries about privacy issues
- managing privacy complaints
- assisting in the preparation of Privacy Impact Assessments (PIAs) (see section 10 of this guideline below)
- maintaining the AFP's register of PIAs
- annually measuring and documenting the AFP's performance against the PMP
- liaising with the OAIC and other agencies on behalf of the AFP in relation to privacy issues.

- **Internal queries**
- AFP appointees should consult the AFP National Guideline on information management and Information Management Handbook or contact the Privacy Officer (via AFP Legal) for privacy advice. For example, advice may be sought on:
- handling personal information
- privacy issues related to new or enhanced functions
- requesting advice from the OAIC
- any proposed changes to privacy obligations.
- The Privacy Officer may consult with relevant areas of the AFP as required. **External queries** All external privacy queries should be directed to the Privacy Officer (via AFP Legal), particularly where a member of the public has:
- a privacy issue in relation to a service provided by the AFP
- expressed a privacy concern about the actions of AFP appointees
- a privacy enquiry relating to how their information is being used by the AFP.
- The OAIC will normally refer all AFP privacy matters to the Privacy Officer; however, if AFP appointees receive any enquiries from the OAIC they must be referred to the Privacy Officer (via AFP Legal).

9. Privacy Champion

- The AFP's Chief Operating Officer is the designated Privacy Champion. Under the Privacy Code, the functions of the Privacy Champion are to
- promote a culture of privacy within the AFP that values and protects personal information
- provide leadership on broader strategic privacy issues
- review and approve the PMP
- report to the AFP's executive in relation to any privacy issues and the AFP's performance against the PMP.

10. Privacy threshold assessments and privacy impact assessments

- The Privacy Code requires the AFP to conduct privacy impact assessments (PIAs) for all new or changed projects with a high privacy risk.
- A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing avoidable impacts or risks, and how they can be removed or reduced to a more acceptable level.
- To determine whether a new project has a high privacy risk and requires a PIA to be conducted, AFP appointees should conduct a privacy threshold assessment (PTA), in accordance with the template and guidance provided in the Better Practice Guide on assessing and managing privacy impacts of AFP projects.
- If a new or changed project does not involve the handling of personal information, a PTA is not required.

- All populated PTA templates must be sent to AFP Legal for assessment by its Privacy Team. The Privacy Team will engage with the project owner as needed to identify any privacy risks that may arise and provide guidance on how to mitigate those risks. In the event that the PTA establishes a project is high risk, the Privacy Team will advise the project owner that a PIA is required.
- If a PIA is not required, the project owner must keep a copy of the completed threshold assessment as a record of the consideration of privacy impacts relevant to the project.
- If a PIA is required, it must be completed by the project owner using the template and guidance provided in the Better Practice Guide on assessing and managing privacy impacts of AFP projects and the resources on the OAIC website. Some projects will have substantially more privacy impact than others, and in some cases, a robust and independent PIA conducted by external assessors may be preferable. Populated PIA templates should be submitted to AFP Legal to the Privacy Team who will conduct or arrange for an assessment.
- Finalised PIAs must be recorded in the AFP's internal PIA register which is maintained by the Privacy Officer. A version of the PIA register is published on the AFP website, in accordance with the Privacy Code requirements.
- If the AFP is working with another agency on a project, the agencies may conduct a joint PIA. The AFP must retain a copy of any joint PIA.

11. Privacy complaints

- Individuals may make a complaint to the AFP or the OAIC about the handling of their personal information. Section 13 of the Privacy Act sets out the acts and practices that may be an **interference with the privacy of an individual**. These include a breach of:
- an APP or a registered APP Code (such as the Privacy Code)
- rules under section 17 of the Privacy Act in relation to tax file number information
- a provision of Part IIIA of the Privacy Act
- prescribed Notifiable Data Breach Scheme requirements.
- AFP appointees must not deal directly with the OAIC in relation to any privacy complaint, and unless the Privacy Officer has advised otherwise, must refer any inquiries to the Privacy Officer (via AFP Legal).
- AFP appointees dealing with a member of the public who raises a privacy issue which could be a complaint under the Privacy Act should both:
- give them the public facing contact details of the Privacy Officer (privacy@afp.gov.au) and suggest they write to the Privacy Officer to outline how they believe their privacy has been breached
- advise the Privacy Officer by email or telephone of the potential complaint.
- The Privacy Officer may consult Professional Standards as some privacy complaints may be best resolved using the Professional Standards Framework.
- If the complaint involves an AFP practice issue, then the matter should be dealt with in accordance with:
- Part V of the AFP Act
- CO2

- AFP National Guideline on complaint management and resolution of grievances.
- Privacy complaints about the AFP may also be made directly to the OAIC. The OAIC will normally liaise with the Privacy Officer about the appropriate handling of these complaints.

12. Notifiable Data Breach Scheme

- The Notifiable Data Breach Scheme (NDB Scheme) in Part IIIC of the *Privacy Act 1988* requires the AFP to notify affected individuals and the Australian Information Commissioner about 'eligible data breaches'. The primary purpose of the NDB Scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm.
- An 'eligible data breach' arises when:
- there is **unauthorised access** to, **unauthorised disclosure** of, or **loss** of, personal information that the AFP holds
- and
- serious harm is likely to occur to one or more individuals
- and
- the AFP has not been able to prevent the likely risk of serious harm with remedial action.
- Incidents that satisfy these three criteria may also give rise to an AFP security incident. AFP personnel must report in accordance with the AFP National Guideline on personnel security as soon as practicable after they become aware of a reportable event or circumstance. All AFP personnel must report security incidents by completing and submitting a Security Incident Report.
- In addition to any other obligation an AFP appointee may have in the circumstances of a data breach, the AFP appointee must also contact the AFP's Privacy Officer (via AFP Legal) to ensure the AFP complies with its obligations under the NDB Scheme, including under Part IIIC of the *Privacy Act 1988*. AFP Legal will also advise if the breach is an eligible data breach.
- There are exceptions to the NDB Scheme that may apply to certain activities or classes of information. For example, an enforcement body does not need to notify individuals about an eligible data breach if its chief executive officer believes on reasonable grounds that notifying individuals would be likely to prejudice an enforcement related activity conducted by, or on behalf of, the enforcement body. The Privacy Officer can provide advice on these aspects of the NDB Scheme.
- Further guidance on the NDB Scheme is available on the OAIC website, including the guidance titled: Data breach preparation and response — A guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth).

13. Further advice

- Queries about the content of this guideline should be referred to AFP Legal.

14. References

- **Legislation**
- *Australian Federal Police Act 1979* (Cth) (the Act)
- *Australian Information Commissioner Act 2010* (Cth)

- *Freedom of Information Act 1982* (Cth)
- *Privacy Act 1988* (Cth)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)
- Privacy (Australian Government Agencies – Governance) APP Code 2017 (Cth)
- **OAIC Guidance**
- Australian Privacy Principles guidelines
- Australian Privacy Principles quick reference tool
- Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)
- **DHA Guidance**
- Protective Security Policy Framework (PSPF)
- **AFP governance instruments**
- AFP Commissioner's Order on professional standards (CO2)
- AFP National Guideline on complaint management and resolution of grievances
- AFP National Guideline on Freedom of Information releases
- AFP National Guideline on information management
- AFP National Guideline on information security
- 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 personnel security
- Information Management Handbook
- Better Practice Guide on assessing and managing privacy impacts of AFP Projects
- AFP Privacy Policy

15. Shortened forms

AFP	• Australian Federal Police
• **APP**	• Australian Privacy Principle
• **FOI**	• Freedom of Information
• **NDB Scheme**	• Notifiable Data Breach Scheme

• **OAIC**	• Office of the Australian Information Commissioner
• **PIA**	• Privacy Impact Assessment
• **PMP**	• Privacy Management Plan
• **PSPF**	• Protective Security Policy Framework
• **the Act**	• *Australian Federal Police Act 1979* (Cth)
• **Privacy Act**	• *Privacy Act 1998* (Cth)
• **Privacy Code**	• *Privacy (Australian Government Agencies – Governance) APP Code 2017*
• **FOI Act**	• *Freedom of Information Act 1982* (Cth)

16. Definitions

- **AFP appointee** is defined in the AFP Glossary.
- **AFP functions** are prescribed by s. 8 of *the Act*
- **AFP practices issue** is defined in s. 40RI of *the Act* as an issue regarding the practices or procedures of the AFP (whether those practices or procedures are carried out within or outside Australia).
- **Eligible data breach** is defined in the *Privacy Act*and means a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.
- **Enforcement body** is defined in s. 6 of the *Privacy Act*, and includes the AFP.
- **Enforcement related activities** is defined in s. 6 of the *Privacy Act* and means the:
- prevention, detection, investigation, prosecution or punishment of:
    - criminal offences
    - breaches of a law imposing a penalty or sanction
- conduct of surveillance activities, intelligence gathering activities or monitoring activities
- conduct of protective or custodial activities
- enforcement of laws relating to the confiscation of the proceeds of crime
- protection of the public revenue
- prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the privacy regulations
- preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.

- **Government related identifier** is defined in s. 6 of the *Privacy Act* mean an identifier of an individual that has been assigned by any of the following:
- an agency
- a state or territory government authority
- an agent or provider acting in their capacity as:
    - an agent of an agency or a state or territory authority
    - a contracted service provider for a Commonwealth, state or territory contract.
- **Office of the Australian Information Commissioner** means the office (including information officers and staff) established by the *Australian Information Commissioner Act 2010*(Cth).
- **Personal information** is defined in s. 6 of the *Privacy Act*, and is further outlined in s. 5 and Attachment 2 of this guideline.
- **Privacy Code** means the Privacy (Australian Government Agencies – Governance) APP Code 2017 (Cth).
- **Project** means:
- new or changed systems, databases, activities, processes or programs, including:
    - a free trial or online application (even where no download or installation of software on AFP systems is not required)
    - investigative technology
- new or altered methods of service delivery or storing information, and
- new or amended legislation or policy proposals.
- **Sensitive information** is defined in s. 6 of the *Privacy Act*, and is further outlined in s. 5 and Attachment 2 of this guideline.

17. Attachments

- Attachment 1 – Australian Privacy Principle 2—anonymity and pseudonymity
- Attachment 2 – Australian Privacy Principle 3—collection of solicited personal information
- Attachment 3 – Australian Privacy Principle 5—notification of the collection of personal information
- Attachment 4 – Australian Privacy Principle 6—use or disclosure of personal information
- Attachment 5 – Australian Privacy Principle 8—cross-border disclosure of personal information