Australian Government
Office of Parliamentary Counsel

Privacy Management Policy

Policy number: 2.13

Document release: 3.0

Date of issue: April 2026 **Next Review**: April 2027

Introduction **2**
Personal and sensitive information **2**
Collection of personal information **3**
Anonymity or pseudonymity **4**
Notification of collection of personal information **4**
Storage of personal information **4**
Disposal of personal information **5**
Disclosure of personal information **5**
Accessing and correcting personal information **6**
Governance **6**
Complaints **7**
Contact Us **8**

Introduction

1) The Office of Parliamentary Counsel (***OPC***) has a central role in supporting Australia's legislation development. We are trusted to act in the best interests of the Australian community and we take our stewardship responsibilities seriously. Our mission is to provide clear, effective and accessible Commonwealth law for all Australians.

2) We take privacy seriously and make all efforts to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure. We are committed to managing personal information in an open and transparent way, and privacy compliance is considered when designing systems and practices. We commit to continual monitoring to improve our privacy compliance.

3) The purpose of this Privacy Management Policy (*the* ***Policy***) is to set out how personal information held by us is managed and protected in compliance with the *Privacy Act 1988* (Cth) (***Privacy Act***), the Australian Privacy Principles (***APPs***) and the Privacy (Australian Government Agencies – Governance) APP Code 2017 (*the* ***Code***).

4) This policy applies to all who are employed or engaged by us (***OPC staff***), including employees, contractors or labour hire, and covers all our activities. All our staff must understand their responsibilities to uphold the standards set out in this policy.

Personal and sensitive information

5) We may collect, use, hold and disclose personal information that is reasonably necessary, or directly related to, the performance of our functions and activities. This may include:

- names and signatures
- personal contact details such as address, email address, phone number
- proof of identity documents
- next of kin contact information
- information about citizenship, visa status and visa application details
- gender
- dates and places of birth
- photographs of people
- facial recognition
- travel arrangement details
- Tax File Numbers
- CVs, employment history, transcripts and referee reports
- financial information provided by contractors and consultants
- bank details where we are required to make payments
- information about individuals subject to financial sanctions and travel bans, including information about financial activities and transactions

- child exploitation and abuse notifications under the Australian Government's Child Protection Policy
- IP address and email address when responding to online comments or enquiries

6) We may also collect sensitive information that is reasonably necessary, or directly related to, the performance of our functions and activities. This may include:

- race or ethnicity
- health information, for example an individual's medical history and any disability or injury that an individual may have
- criminal history, religious beliefs, philosophical beliefs, political opinions or associations, for example when provided by individuals as part of a security assessment process

7) In this policy, ***personal information*** and ***sensitive information*** have the meaning given to these terms in the Privacy Act.

We must not adopt a government-related identifier as its own identifier for an individual, or use or disclose such an identifier, unless:

- required or authorised by law;
- it is reasonably necessary to verify a person's identity; or
- it is otherwise permitted under the Privacy Act.

Collection of personal information

8) We collect personal information only by lawful and fair means. We will only collect your personal information directly from you or your authorised representative. This may be via telephone, letter, email, face-to-face or online.

9) Where we receive personal information that it has not actively sought, we will determine whether the information could have been collected in accordance with the Privacy Act. If the information could not have been lawfully collected, we will take reasonable steps to destroy or de-identify the information as soon as practicable, where lawful and reasonable to do so. Where the information could have been lawfully collected, we will manage the information in accordance with this Policy and the Australian Privacy Principles.

10) We may collect and store sensitive information about you with your express or implied consent, where the collection and storage is required or authorised by law or where we are otherwise permitted under the Privacy Act, or where it is required to manage our functions. Our functions include:

- drafting Commonwealth Bills and legislative, notifiable and other instruments
- publishing legislation, including maintaining the Federal Register of Legislation
- training APS officers in drafting and publishing legislation

Anonymity or pseudonymity

11) You have the option to interact anonymously or using a pseudonym when interacting with us. For example, if you contact us with a general question, you will not be required to give your name unless it is required to adequately handle your enquiry.

12) However, for some interactions where we are required or authorised to deal specifically with you by or under law, or where it is impracticable for us to deal with you anonymously or pseudonymously, this option will not be available to you. This may include when you apply for employment, or providing enough personal information about your particular matter to enable us to deal with your matter fairly and efficiently.

Notification of collection of personal information

13) Where we collect personal information about you, we will take all reasonable steps either to notify you of certain matters or to ensure you are aware of those matters. We will take all reasonable steps to do this before, or at the time we collect your personal information. If this is not practicable, we will take all reasonable steps to notify you as soon as practicable after collection.

14) When giving you notice of collection of your personal information, we must notify you of the following:

- OPC's identity and contact details;
- the fact and circumstances of collection;
- whether the collection is required or authorised by law;
- the purposes of collection;
- the consequences if personal information is not collected;
- our usual disclosures of personal information of the kind collected by us;
- information about our Privacy Management Policy;
- whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

15) For each item above, we may decide not to notify you in reasonable circumstances, for example, where something is obvious.

Storage of personal information

16) Personal and sensitive information held by us in Commonwealth records (other than information stored in the Federal Register of Legislation) is managed securely through our business systems. We take physical and electronic security measures to protect your personal and sensitive information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

17) Our electronic records management system, network drives and virtual server environment are hosted by us within Australia. We secure electronic information using firewalls, secure databases, secure online systems, password protection for electronic files, and multi-factor authentication.

18) We restrict physical access to offices and secure physical files using secure cabinets and containers.

19) Our staff have access to personal and sensitive information on a need to know basis only. Your personal and sensitive information stored in our databases can only be accessed by authorised users to work on particular enquiries, complaints, applications, and/or cases. Our databases have an audit trail whenever personal information is included, amended, or deleted.

Disposal of personal information

20) We will take reasonable steps to destroy or de-identify your personal information we hold once your personal information is no longer needed for any purpose for which your personal information may be used or disclosed under the APPs.

21) When no longer required to be retained as part of a Commonwealth record, your personal and sensitive information may be destroyed. Any destruction of your personal or sensitive information will be made in accordance with the *Archives Act 1983*.

22) This requirement does not apply where your personal information is contained in a Commonwealth record or where we are required by law or a court/tribunal order to retain your personal information.

Disclosure of personal information

23) We will generally only use your personal or sensitive information for the primary purpose for which it was collected. For example, to assess your employment application or to respond to your enquiry.

24) We do not use personal or sensitive information for direct marketing purposes.

25) We may also use or disclose your personal information in accordance with the Privacy Act, including where:

- You have consented to use or disclosure for a secondary purpose.
- You would reasonably expect your information to be used or disclosed for a secondary purpose which is related to the primary purpose, or in the case of sensitive information, where the secondary purpose is directly related to the primary purpose.
- it is required or authorised by or under law.
- it is reasonably necessary for an enforcement activity conducted by or on behalf of an enforcement body. For example, if you are suspected of committing fraud or corruption against the Commonwealth, we will disclose your personal information to an enforcement body for investigation.

26) We may use or disclose personal information, or engage third parties to collect personal information on our behalf, where this is reasonably necessary for the performance of our functions. We will take reasonable steps to ensure that

appropriate privacy protections are in place in accordance with the Privacy Act. Disclosure may occur to:

- suppliers and other third parties with whom we have commercial relationships;
- any organisations for any authorised purpose that directly relates to one of our functions, with the individual's express consent; or
- other relevant vendors contracted to assist us to perform our functions.

27) We will not disclose your personal or sensitive information to any overseas recipients unless one of the following applies:
- You have consented to the disclosure after being expressly informed that we will not be responsible for the overseas recipient's handling of your personal information;
- it is required or authorised by or under law;
- it is required or authorised by an international agreement relating to information sharing to which Australia is a party;
- it is reasonably necessary for an enforcement related activity conducted by, or on behalf of, an enforcement body and the recipient performs similar functions.

Accessing and correcting personal information

28) You have the right to ask for access to your personal information that we hold about you, and to ask that it is corrected. You can ask for access or correction by contacting us on the details below. Once contacted, we must respond to your request within 30 days.

29) If asked, we must give you access to your personal information and take reasonable steps to correct it if we agree that it is incorrect, unless there is a law that allows or authorises or requires us not to. Upon a request for access or correction being made, we will ask to verify your identification before giving you access to personal information or the ability to correct it. We will make this process as simple as possible. If we refuse your access or correction request, we must notify you in writing setting out our reasons for doing so.

30) The steps appropriate to verify your identity will depend on the circumstances. We will seek the minimum amount of your personal information needed to establish your identity.

31) You also have the right under the *Freedom of Information Act 1982* to request access to documents that we hold and ask for information that we hold about you to be changed or annotated if it is incomplete, incorrect, out-of-date or misleading.

Governance

32) **Personal information holdings register**. We maintain a Personal Information Holdings register which is updated as required.

33) **Privacy management plan**. We have a Privacy Management Plan (PMP) which identifies specific, measurable privacy goals and targets and sets out how we will meet our compliance obligations under the APPs.

The PMP will also assess whether we use automated or computer-based decision-making involving personal information and ensure transparency obligations under APP 1 are met if such practices are introduced.

34) **Privacy impact assessment**. We will conduct a Privacy Impact Assessment (PIA) for significant new projects in which personal information will be handled, or when a significant change is proposed to information handling practices. This is used to identify the impact that this activity might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

35) **Privacy risk management**. We conduct assessments on the risks associated with collecting, storing, using, disclosing and destroying personal and sensitive information.

36) **Notifiable data breach**. We must take reasonable steps to protect your personal information from misuse, interference, loss and unauthorised access, modification or disclosure. We will notify individuals as well as the Information Commissioner in the event of certain data breaches. The purpose of notification is to ensure that you know if your personal information is involved in a suspected breach. This enables you to proactively minimise the potential harm to you by changing passwords on compromised accounts and being aware of the risk of identity fraud.

Complaints

37) We take privacy seriously and will make all efforts to protect your personal information from misuse, interference, and loss; and from unauthorised access, modification or disclosure.

38) You can make a complaint about how we deal with your personal information by contacting us on the details below. To assist us to gather relevant information about a complaint, we will need as much information as possible in describing how your privacy has been interfered with, including:

- What happened
- When it happened (including dates)
- What personal information was affected
- Who did it (include individual names if known)
- How and when it was discovered
- Contact details
- Any other relevant information, including what, if any, outcomes are expected from the complaint process.

39) If the alleged privacy breach involves personal information which does not belong to you, we will ask for evidence that you have authority to act on behalf of the person before proceeding any further.

40) We will provide you a written response to the complaint. If a breach of the APPs has been identified as a result of a complaint, we will advise you of the findings within 30 days.

Contact Us

41) You can make an enquiry or complaint about how we have handled your personal information, or if you wish to request access or correction to your personal information, or you have questions or comments about this privacy policy, please email privacy@opc.gov.au.

42) You may also write to:

Privacy Officer
Corporate Services Branch
Office of Parliamentary Counsel
Locked Bag 30
Kingston ACT 2604