Australian Government
Department of Home Affairs



AI Transparency Statement

February 2025

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Table of Contents

Introduction **2**

What is Artificial Intelligence? 2
Accountable Officials 2
Domains of AI Usage 2
AI Governance 3

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Introduction

The Digital Transformation Agency (DTA) *Policy for the responsible use of AI in government* (the policy) mandates all departments and agencies to designate accountable officials for the policy implementation, and to publish a statement outlining their approach to AI adoption and use ('transparency statement').

The Department of Home Affairs (the department) is responsible for providing services, policy, and regulation across a range of domains including immigration and border protection, citizenship, cyber and national security. In delivering its role effectively and efficiently, the department incorporates the safe and responsible use of data and enabling technologies including various forms of Artificial Intelligence (AI).

What is Artificial Intelligence?

Following the DTA, the department adopts the Organisation for Economic Co-operation and Development (OECD) definition of an AI system:

'An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.'

Accountable Officials

The Chief Data Officer (CDO) is the Accountable Official for AI under the policy and responsible for leading the department's data and AI program. This includes improving AI literacy, policy monitoring and improvement, robust and ethical AI design and management, and implementation of governance and assurance mechanisms for AI adoption in the secure and safe technology environments provided by Information Communication Technology (ICT).

Domains of AI Usage

The department embraces opportunities presented by emerging technologies by developing and adopting AI systems in support of decision-making, risk mitigation and management, and administrative actions in a safe and responsible manner. The department uses AI to boost productivity by optimising processes across various domains:

- Service Delivery: with a range of systems to improve efficiency of department's service to clients such as automated registration of submissions and applications; or image processing systems to facilitate passenger movements.
- Law Enforcement, Intelligence and Security: the trained AI systems use advanced analytics for insights to inform a data-driven approach to risk identification, intelligence gathering and crime prevention.
- Corporate and Enabling: the explorative use of AI systems to support administrative tasks and research leading to faster generation of products for internal use such as feedback analysis of large surveys to derive key learnings that enable organisational growth and transformation.
- Compliance and Fraud Detection: AI systems are used to identify and share information with partners to supplement compliance activities, keeping the Australian community safe and ensuring the integrity of Australia's migration program.

The department uses both internal and third party AI systems, with ongoing human monitoring and decision making to ensure AI use is safe, legal and ethical.

Released by Department of Home Affairs under the Freedom of Information Act 1982

AI Governance

The department is committed to transparency and accountability in using AI, ensuring responsible implementation as the technology evolves.

To ensure safety, security and ethical use of its AI systems, the department has implemented a number of controls for governing, monitoring and managing AI-related risks by:

- aligning *Home Affairs' AI Ethics Policy* with *Australia's AI Ethics Principles,* and making the policy compliant with both international and Australian human rights legislation, such as *Racial Discrimination Act 1975*, *Australian Human Right Commission Act 1986* and *International Covenant on Economic, Social and Cultural Rights*
- implementing processes and procedure, to enable continuous and transparent improvement of AI systems
- embedding human monitoring, verification, and intervention on all AI system-generated outputs
- monitoring and mitigating AI distinct and specific risks and potential harms to privacy, fairness, transparency and explainability as well as safety and security of its technology environments
- delivering a comprehensive data and AI literacy program to its workforce.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Privacy policy (homeaffairs.gov.au)

Privacy policy

1. Introduction
2. The kinds of personal information we collect and hold
3. How we collect your personal information
4. The purposes for which we collect, hold, use and disclose your personal information
5. How we hold personal information
6. Access, correction and complaints
7. Additional information

---

1. Introduction

This privacy policy explains how the Department of Home Affairs, including the Australian Border Force (the Department), manages the personal information it collects. It also outlines the information flows associated with that personal information.

This privacy policy is an overview. It does not provide details about all of our personal information management practices, procedures and systems. You can find more information at Section 7 – Additional information. This includes a link to the Department's Privacy Notice – Form 1442i.

Outline of this policy:

1. Introduction
    - Our role
    - Our obligations under the Privacy Act
    - Privacy Impact Assessment Register
2. The kinds of personal information we collect and hold
3. How we collect your personal information
4. The purposes for which we collect, hold, use and disclose your personal information
    - Enforcement Related Activities and Law Enforcement Purposes
    - Additional disclosure purposes

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- Disclosure of personal information to overseas recipients

5. How we hold personal information
   - Storage and data security
   - Visits to our website
6. Access, correction and complaints
   - Data Quality
   - Access to personal information
   - Correction of personal information
   - Complaints
7. Additional information

The Department values your privacy and takes its obligations under the *Privacy Act 1988* (Privacy Act) seriously. We are committed to treating your personal information as a valuable business asset to be respected, managed and protected. The Department implements a 'privacy by design approach'. We have senior departmental officers with overall accountability for privacy: our Privacy Officer and Privacy Champion.

Our role

Our key objectives are to:

1. protect Australia from national security and criminal threats through:
   - cyber and critical infrastructure resilience and security
   - immigration
   - border security and management
   - counter-terrorism
   - the protection of our sovereignty
   - citizenship and social cohesion.
2. support a prosperous and united Australia through effective coordination and delivery of immigration and social cohesion policies and programs
3. advance a prosperous and secure Australia through trade and travel facilitation and modernisation, and effective customs, immigration, maritime and enforcement activities across the border continuum.

Our obligations under the Privacy Act

This privacy policy sets out how we comply with our obligations under the Privacy Act. The Privacy Act sets out 13 Australian Privacy Principles (APPs). These regulate the collection, use, disclosure and storage of personal information and how individuals can access and correct personal information held about them. We are legally bound by the APPs and the Australian Government Agencies Privacy Code (the Privacy Code).

The Privacy Act defines personal information as:

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- *whether the information or opinion is true or not; and*
- *whether the information or opinion is recorded in a material form or not.*

The Privacy Act also requires the Department to notify an individual of certain matters when we collect personal information about them. The Department's Privacy Notice – Form 1442i, or specific privacy notices where collection is beyond the scope of Form 1442i, provides further notification of those matters.

Privacy Impact Assessment Register

In accordance with section 15(1) of the Privacy Code, the Department is required to maintain a Privacy Impact Assessment (PIA) Register of all PIAs completed since 1 July 2018.

You can find details of the PIAs the Department has completed on the PIA Register.

2. The kinds of personal information we collect and hold

This section outlines the kinds of personal information that the Department collects and holds. The Department collects both personal and sensitive information. Sensitive information is a subset of personal information (explained above). The Privacy Act defines sensitive information as:

- information or an opinion, that is also considered personal information, 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 orientation or practices
    - criminal record
- health information about an individual
- genetic information about an individual that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification or
- biometric templates.

Sensitive information is generally afforded a greater level of protection under the Privacy Act.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Privacy policy (homeaffairs.gov.au)

The type of information collected will vary depending on the purpose for collection. These purposes for collection are discussed at Section 4 – The purposes for which we collect, hold, use and disclosure your personal information. Broadly, the types of information collected includes, but is not limited to:

- name
- date of birth
- gender
- contact details such as address, email address and telephone numbers
- country of residence or citizenship
- country of birth
- ethnicity
- religion
- main language and English/reading proficiency
- passport/travel document number, country and expiry date
- visa grant details
- employment status, occupation/career history and qualifications.
- years of schooling, years of further education
- enrolment details
- family details/history
- health details
- medical reports, x-ray images
- criminal history
- personal identifiers such as fingerprint images and facial images
- copies of any identity documents
- financial details
- information for the purpose of determining age
- refugee status/background, months in refugee camp, any associated medical alert, torture/trauma issues, and protection claims
- interpreter requirements
- relationship status
- passenger name record information including flight/vessel details, port code
- visa subclass and expiry date
- information and intelligence from other government agencies, organisations and foreign governments
- allegations
- information obtained through warrants
- foreign immigration intelligence
- surveillance reports
- interview reports from third parties
- security assessment
- care plan notes
- incidents and visitor information
- staff information including biographical details, tax file number, next of kin, information related to security clearance, staff development, training details, medical information, compensation details, salary/payment details and details of accounts with financial institutions

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- information relating to our website access such as IP or server address, the date and time of the visit to the site, pages accessed, operating system, web browser version and type, time taken to transmit information to the person, previous internet address from which the person came directly to this website.

The Department also collects and holds Electronic Monitoring information for the purposes of compliance with the *Migration Amendment (Bridging Visa Conditions) Act 2023* (Cth).

3. How we collect your personal information

We only collect personal information for purposes reasonably necessary for, or directly related to, the Department's functions or activities, pursuant to the Administrative Arrangements Orders and portfolio legislation. This includes, but is not limited to, the *Australian Citizenship Act 2007*, the *Customs Act 1901* and the *Migration Act 1958.*

Individuals have the option of dealing anonymously or by pseudonym with the Department (APP 2). However, this may not be possible where the Department is required or authorised by law or a court or tribunal order to deal with identified individuals, or it is impracticable for the Department to deal with individuals who have not identified themselves.

Our usual practice is to collect personal information directly from the individual or their authorised representative. We may collect this information through interviews, application forms and other official forms.

We often also collect personal information from other sources. These include third parties or publicly available sources. Third parties include:

- other Australian government agencies
- law enforcement agencies
- foreign governments
- sponsors
- medical practitioners
- organisations that a person has nominated
- education providers
- employers
- members of the public who contact us with information.

If clients are concerned about the inherent risks associated with transmission of information over the internet, we can communicate with them through other avenues. Online, all interactions between clients and us are protected by an industry standard 128-bit SSL encryption technology. We employ firewall technology to help to protect our internal systems and personal information against intrusion from the internet.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

We also use Qualtrics, a third party software supplier to administer online surveys. These help us improve our services. Access to survey response data is tightly controlled and restricted to nominated departmental personnel. Data collected by Qualtrics is securely collected and managed onshore in Australia. This is in accordance with their privacy statement.

You can find more information on the storage and security of the personal information we hold at Section 5 – How we hold personal information.

4. The purposes for which we collect, hold, use and disclose your personal information

We are authorised under our portfolio legislation to collect, use and disclose a range of personal information. This legislation includes, but is not limited to, the:

- *Australian Border Force Act 2015*
- *Australian Citizenship Act 2007*
- *Customs Act 1901*
- *Migration Act 1958*
- Privacy Act.

We will use or disclose personal information (including sensitive information) for the purposes for which it was collected, and for secondary purposes where permitted by law.

Our primary purpose when collecting personal information is to carry out our functions and activities. We manage the following programs:

- visa and migration
    - including processing visa claims and migration applications
- customs and excise
- certain Australian laws including:
    - taxation
    - health
    - quarantine
    - commerce
    - criminal
    - intellectual property
    - community protection.
- refugee and humanitarian assistance and programmes. These include the humanitarian programme outside Australia and protection programme in Australia
- border management including:
    - facilitating the entry of genuine travellers to Australia while preventing entry of those likely to threaten Australia's national interests
    - explaining the need for identity, health, character and security checks

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

    - recording the arrivals and departures of travellers and goods to and from Australia (movement records)
    - facilitating the transfer and recording of goods over the Australian border.
- visa compliance and immigration status resolution including the:
    - detection and location of persons who have no lawful authority to be in Australia or people in breach of their visa condition(s)
    - cancellation or refusal of visas to non-citizens who might be of concern to the public. This could be for reasons such as involvement in serious criminal activity.
- immigration detention, removal or transfer to a regional processing country. This includes working with service providers and foreign authorities in support of offshore processing, such as law enforcement, as well as the provision of welfare services and settlement
- citizenship, including the assessment of applications.

We also conduct the following administrative activities:

- processing freedom of information (FOI) requests under the *Freedom of Information Act 1982* (FOI Act), privacy requests under the Privacy Act, and administrative access requests
- staffing and personnel related activities
- complaint handling procedures, including complaints lodged with:
    - the Ombudsman's Office
    - Office of the Australian Information Commissioner (OAIC)
    - Australian Human Rights Commissioner
    - our Global Feedback Unit.
- maintaining our website.

We use personal information for a secondary purpose where reasonably necessary for enforcement-related activities conducted by or on behalf of the Department (or another enforcement body). We may also use the information in circumstances where a person would reasonably expect us to use it for a secondary purpose. This can be either directly related to the primary purpose (for sensitive information) or related to the primary purpose (for other personal information). For example, the information provided for the primary purpose of processing one visa or citizenship application can be used for the secondary purpose of subsequent applications.

Enforcement Related Activities and Law Enforcement Purposes

In understanding our ability to collect, use and disclose personal information under the Privacy Act, it is important to be aware that we are an enforcement body for the purposes of the Privacy Act.

As an enforcement body, we can collect, use and disclose personal information (including sensitive information) where it is reasonably necessary for, or directly

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

related to, one or more enforcement related activities conducted by or on behalf of us (or another enforcement body).

Enforcement related activities of the Department include, but are not limited to:

- detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law
- identifying and locating unlawful non-citizens and resolving their immigration status. This includes the removal of unlawful non-citizens from Australia
- preventing and reducing illegal migration, people smuggling and trafficking in persons
- identifying and assessing claims by non-citizens for protection in Australia. This includes managing the detention or release into the community of protection claimants
- assessing and enforcing compliance with visa and citizenship requirements
- identifying and assessing prior to arrival those entitled to lawfully enter Australia
- managing the entry and departure of people crossing the Australian border
- resolving the identity, health, national security and criminal history status of people applying to enter Australia
- collecting information to assess the identity, character and criminal history of applicants for Australian citizenship
- cooperation with other agencies, including information-sharing, for law enforcement and border security purposes, and the protection of public revenue.

We are permitted to disclose personal information to law enforcement bodies (amongst others) and intelligence bodies for the purpose of enforcing the criminal law, laws imposing a pecuniary penalty or for the purpose of protecting public revenue (amongst other things). Usual disclosures include to:

- Australian and overseas law enforcement bodies to assess character issues
- Australian and overseas law enforcement bodies and intelligence agencies or commissions, National Common Police Services, Interpol, regulatory commissions, parliamentary commissions of inquiry, international tribunals and overseas immigration authorities, to identify or investigate immigration fraud, national security issues, or suspected involvement in international crimes such as war crimes, crimes against humanity or genocide
- the Australian Federal Police, under information-sharing agreements
- the Australian Taxation Office, Centrelink and other Commonwealth or State and Territory agencies, to assist the enforcement of immigration or visa conditions
- the Australian Taxation Office and Australian police forces to locate unlawful non-citizens
- the Director of Public Prosecutions prosecuting migration or citizenship offences
- foreign governments for the removal of an unlawful non-citizen or transfer to a Regional Processing Country

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- registered educational institutions, employers, sponsored persons, sponsors and labour suppliers to monitor compliance with visa conditions and sponsorship obligations, and notify instances of sanctions imposition.

Additional disclosure purposes

In addition to disclosures for the primary purpose of collection and for enforcement related activities, the Department may also disclose your personal information for the following purposes, including but not limited to:

- other government agencies to:
  - confirm identity
  - verify the authenticity of documents provided
  - undertake data matching
  - manage compliance obligations
  - obtain information where their portfolio legislation provides them with a power under an Australia law to obtain certain personal information
- keep your nominated representatives informed. This could include:
  - a family member
  - a migration agent
  - your travel agent
  - airlines
  - Ombudsman
  - Member of Parliament
  - solicitor
- facilitate merits or judicial review of a decision
- assess suitability to hold a professional licence by disclosing information to licensing authorities about migration status and work
- where it is authorised by portfolio legislation including but not limited to the *Australian Border Force Act 2015*, the *Australian Citizenship Act 2007*, the *Customs Act 1901* and the *Migration Act 1958*
- where contact details may be provided to Australian law enforcement bodies or emergency services in the event of an emergency, serious injury or death
- Centrelink to facilitate release of bonds paid or identification and recovery of debts incurred
- for employment, labour supply and business skills. This includes to employers, labour suppliers and third parties who use clients services through a labour supply arrangement. For example, when a person applies for work, we may disclose to the employer or labour supplier information about their eligibility to work. We may also disclose information to state and territory economic development departments and agencies that help business skills migrants access government business information and services
- for training and education. This includes:
  - assisting those seeking to undertake training or education in Australia
  - determining any impact of a proposed workplace component on the Australian labour market
  - to assess overseas qualifications for some classes of visas

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

    - to facilitate English language tuition under the Adult Migrant English Programme
    - to monitor registered training organisations
- for health purposes including:
    - to determine whether the health requirement is met for granting a visa
    - for consideration of whether the health requirement should be waived
    - for management of public health risks
- for the refugee and humanitarian entry and on-shore protection including to the United Nations High Commissioner for Refugees (UNHCR) for the purpose of verifying identity, and humanitarian or protection claims, and the International Organization for Migration to assist its delivery of services
- for detention purposes including State and Territory welfare agencies in relation to detention arrangements, care for unaccompanied minors or detainees with physical and mental health disabilities, state and territory correctional services to facilitate transfers and confirm immigration status, schools, medical practitioners and health and welfare services providers, or migration advisors providing services to detainees or assessing options to assist the detainee. We may also provide personal information concerning people in immigration detention to independent observers contracted to participate in interviews involving minors. These observers are bound by the same privacy obligations that bind us.
- for the welfare and protection of children including:
    - organising and monitoring care and welfare arrangements in immigration detention and/or in the community
    - investigating possible abuse or neglect
    - facilitating travel arrangements and documentation
    - information relating to children entering Australia for adoption may be disclosed to adoptive parents, prospective adoptive parents and state/territory welfare organisations responsible for inter-country adoption issues
    - with regard to children in detention, information may be disclosed to education providers to enable those children to be enrolled in school programs.
- research, evaluations and surveys including to conduct and analyse research, evaluation and surveys about the Department's programs and services, insofar as it adheres to the confidentiality and privacy clauses in our contracts, to facilitate demographic research on new arrivals and analysis of various migration programmes and settlement outcomes and to assist settlement planning or provide settlement services.
    - Our publications do not reveal information that could identify individuals. Where surveys are conducted, we will inform clients of how data will be used. Where research is conducted by a contractor, the contract will include conditions regarding the use and disclosure of information.
- administrative activities including Code of Conduct investigations and injury management.

Disclosure of personal information to overseas recipients

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

We may need to provide your personal information to an overseas recipient as part of our work.

We use contractors to collect, transmit and store data, including providers located outside Australia.

In some circumstances personal information is disclosed to recipients outside Australia. Often the recipient will be the person's country of usual residence or the country the person has departed from (unless the person is awaiting an assessment of protection claims). This will include disclosures to airlines or travel agents in respect of advanced passenger processing and electronic visa processing.

We exchange information with countries or international organisations that have information sharing agreements with Australia. These information exchanges might involve sharing personal identifiers. If there is a match with personal identifiers, we may disclose:

- biographical data
- copies of travel and other identity documents or information from such documents
- immigration status and immigration history (which might include any immigration fraud and offences)
- any relevant criminal history information.

The purpose of such disclosure is to help confirm identity and determine if the person has presented to other agencies under the same identity and with similar claims. The Migration Act imposes limits on the disclosure of identifying information of applicants for protection visas to foreign governments in respect of which the claim is made, unless:

- the applicant has requested or agreed to return to the foreign country
- the person’s application has been refused and finally determined.

5. How we hold personal information

Personal information collected by us is held in electronic databases. Some personal information is also held in paper files.

The databases maintain audit trails whenever personal information in electronic records is accessed, added, amended or deleted on the database.

A departmental record containing personal information can only be destroyed after it has reached its destruction date as identified in a Records Authority issued by the National Archives of Australia. When no longer required, personal information is destroyed in a secure manner, in accordance with Australian Government records management regulations, guidelines and authorities,

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

including the *Archives Act 1983*, Records Authorities and General Disposal Authorities.

Storage and data security

The Commonwealth has developed a Protective Security Policy Framework (PSPF), which includes information security management policies.

The PSPF ensures that:

- all official information is safeguarded to ensure its confidentiality, integrity, and availability by applying safeguards so that:
    - only authorised people, using approved processes, access information
    - information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements
    - information is classified and labelled as required
- all information created, stored, processed, or transmitted in or over government information and communication technology (ICT) systems is properly managed and protected throughout all phases of a system's life cycle. This is in accordance with the protocols and guidelines set out in the PSPF, which includes the Australian Government Information Security Manual, produced by the Australian Signals Directorate.

The following is a brief summary of our current practices and procedures in storing and securing data:

- access to information collected from clients is restricted to authorised persons on a need-to-know basis
- our internal networks and databases are protected using firewall, intrusion detection and other technologies
- applications made using online services and e-services sections of our website are encrypted
- paper files containing sensitive information are protected in accordance with Australian Government Security policy. They are secured in locked cabinets, Australian Government-approved security containers or Secure Rooms with restricted access
- our premises are under 24-hour surveillance. Access is via security passes only, with all access and attempted access logged electronically
- we regularly conduct system audits and staff training. This ensures we adhere to our established protective and computer security practices.

Visits to our website

We log a record of each visit to our site. We record information for statistical purposes and we use it to:

- monitor the use of the site
- discover what information is most and least accessed

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- make the site more useful.

We analyse the information we collect to show broken links on our website, bottlenecks, and other site problems. We use this information to maintain the site for efficient use. We might also collect information about the IT device you use. We could use this information to identify you so we can carry out our functions and activities.

Cookies

We use cookies for maintaining contact with a user through a website session. A cookie is a small file supplied by us, and stored by the web browser software on a person's computer when they access our site. Cookies allow us to recognise people as individual web users as they browse the website.

Our website uses two cookie types - session cookies and persistent cookies.

Session cookies exist only for the duration of a web browser session with a particular website/host. These cookies will be immediately lost when a person ends their internet session or shuts down their computer. Our copy of each user's information will be automatically deleted twenty minutes after they have last used the system. We only use this information to help people use our website systems more efficiently. We do not use the information to track their movements through the internet, or to record personal information about them.

Persistent cookies stay in one of a user's browser subfolders until that person deletes them manually or their browser deletes them based on the duration period contained within the persistent cookie's file. This period is usually beyond the termination of the current session.

No personal information is stored within cookies used by our website. We will not attempt to identify anonymous users or their browsing activities unless legally compelled to do so. This may include where a law enforcement body exercises a warrant to inspect the Internet Service Provider's log files.

6. Access, correction and complaints

Data quality

We take steps to ensure that the personal information we collect is accurate, up-to-date and complete. These steps include correcting personal information, when it is reasonable to do so, that is:

- inaccurate
- out-of-date
- incomplete
- irrelevant
- misleading.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

We conduct regular audits and quality inspections to ensure the accuracy and integrity of information. We check information regularly, and promptly resolve any systemic data quality issues that we identify.

Access to personal information

Individuals can request access to information about themselves in departmental documents under APP 12 of the *Privacy Act* or *Freedom of Information Act 1982* (FOI Act).

For information on how to submit an FOI request, please click here.

Corrections of personal information

Individuals can seek to amend or annotate their personal information. How we amend or annotate a record depends on a number of circumstances.

Australian citizens

Australian citizens seeking to change their personal information on their evidence of Australian citizenship such as name or date of birth should apply to Change a citizenship certificate. They will need to provide the required documents and fee in accordance with instructions on the form.

ImmiCard holders and changes under FOI and Privacy Acts

Applicants can request to change biographic details on an ImmiCard (name or date of birth) by completing an ImmiCard amendment request. Applicants will need to attach official documentary evidence and/or an Australian Government issued Change of Name or Marriage Certificate to support the requested change.

We will consider issuing a new ImmiCard with amended biographic details following assessment of the online request and the evidence provided. The request may be referred to a case manager for an identity assessment as part of the visa process.

Non Australian citizens (permanent and temporary visa holders) with supporting documentation

Where an individual has official documentation in support of an amendment or correction, such as a passport or Australian Government issued Change of Name or Marriage Certificate, they should submit their request in writing using Form 1022 - Notification of Change in Circumstance or Form 1023 - Notification of Incorrect Answers. The individual can submit the form through an ImmiAccount or send it to the nearest departmental office. They will need to include high-resolution scans (600dpi) of certified documentary evidence to support the

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

identity change. An authorised case officer or relevant visa processing area may action the change.

Where the change is not supported by documented evidence

Where an individual's request is not supported by official documentary evidence, and a decision is made under the Privacy Act to refuse correction, the individual can apply under the FOI Act to amend or annotate their personal records. For more information, refer to How to make a FOI request. Under the legislation that governs it, we do not have any power to 'create' a new identity. This includes where a person chooses to change their name. Under Australian law, the State and Territory Registrars of Births, Deaths and Marriages (RBDM) are the responsible authorities for preferred name changes.

Complaints

Making a complaint to us

If a person believes we have wrongly collected or handled their personal information, they can complete an online feedback form.

They can also write to:
The Manager
Global Feedback Unit
GPO Box 241
Melbourne Vic. 3001
Australia

We are committed to a quick and fair resolution of complaints. Every complaint will be investigated and complainants will be advised of the outcome.

Making a complaint to the Office of the Australian Information Commissioner

If a person is unsatisfied with our response, they can write to the Office of the Australian Information Commissioner (OAIC). The OAIC can investigate privacy complaints about the protection of personal information. They can also direct departments to change the way they handle personal information. If a person needs help lodging a compliant with the OAIC, they can call the OAIC Enquiries Line on 1300 363 992. If they are calling from outside Australia, they can call +61 2 9284 9749.

The OAIC can receive privacy complaints through:

- the online Privacy Complaint form on the OAIC's website

by mail to:
GPO Box 5218
Sydney NSW 2001

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- If a person has concerns about postal security, they can consider sending their complaint by registered mail.
- by fax to +61 2 6123 5145
- by email to enquiries@oaic.gov.au. Email that is not encrypted can be copied or tracked.

A person can make a complaint directly to the OAIC rather than to us. It is likely that the OAIC would recommend that a person try to resolve the complaint directly with us in the first instance.

7. Additional information

Additional information about our privacy practices is available from the following sources:

- the Department's Privacy Notice - Form 1442i
- General information about privacy requirements is available from the Office of the Australian Information Commissioner website.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

1. Introduction
2. The kinds of personal information we collect and hold
3. How we collect your personal information
4. The purposes for which we collect, hold, use and disclose your personal information
5. How we hold personal information
6. Access, correction and complaints
7. Additional information

1. Introduction

This privacy policy explains how the Department of Home Affairs, including the Australian Border Force, (the Department) manages the personal information it collects. It also outlines the information flows associated with that personal information.

This privacy policy is an overview. It does not provide details about all of our personal information management practices, procedures and systems. You can find more information at Section 7 – Additional information. This includes a link to the Department's Privacy Notice – Form 1442i.

Outline of this policy:

1. Introduction
    - Our role
    - Our obligations under the Privacy Act
    - Privacy Impact Assessment Register
2. The kinds of personal information we collect and hold
3. How we collect your personal information
4. The purposes for which we collect, hold, use and disclose your personal information
    - Enforcement Related Activities and Law Enforcement Purposes
    - Additional disclosure purposes
    - Disclosure of personal information to overseas recipients
5. How we hold personal information
    - Storage and data security
    - Visits to our website
6. Access, correction and complaints
    - Data Quality
    - Access to personal information
    - Correction of personal information
    - Complaints
7. Additional information

The Department values your privacy and takes its obligations under the *Privacy Act 1988* (Privacy Act) seriously. We are committed to treating your personal information as a valuable business asset to be respected, managed and protected. The Department implements a 'privacy by design approach'. We have senior departmental officers with overall accountability for privacy: our Privacy Officer and Privacy Champion.

Our role

Our key objectives are to:

1. protect Australia from national security and criminal threats through:

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

    - effective national coordination
    - policy and strategy development
    - emergency management
    - regional cooperation
2. support a prosperous and united Australia through effective coordination and delivery of immigration and social cohesion policies and programs
3. advance a prosperous and secure Australia through trade and travel facilitation and modernisation, and effective customs, immigration, maritime and enforcement activities across the border continuum.

Our obligations under the Privacy Act

This privacy policy sets out how we comply with our obligations under the Privacy Act. The Privacy Act sets out 13 Australian Privacy Principles (APPs). These regulate the collection, use, disclosure and storage of personal information and how individuals can access and correct personal information held about them. We are legally bound by the APPs and the Australian Government Agencies Privacy Code (the Privacy Code).

The Privacy Act defines personal information as:

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- *whether the information or opinion is true or not; and*
- *whether the information or opinion is recorded in a material form or not.*

The Privacy Act also requires the Department to notify an individual of certain matters when we collect personal information about them. The Department's Privacy Notice – Form 1442i, or specific privacy notices where collection is beyond the scope of Form 1442i, provides further notification of those matters.

Privacy Impact Assessment Register

In accordance with section 15(1) of the Privacy Code, the Department is required to maintain a Privacy Impact Assessment (PIA) Register of all PIAs completed since 1 July 2018.

You can find details of the PIAs the Department has completed on the PIA Register.

2. The kinds of personal information we collect and hold

This section outlines the kinds of personal information that the Department collects and holds. The Department collects both personal and sensitive information. Sensitive information is a subset of personal information (explained above). The Privacy Act defines sensitive information as:

- information or an opinion, that is also considered personal information, about an individual's
    - racial or ethnic origin
    - political opinions
    - membership of a political association

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

    - religious beliefs or affiliations
    - philosophical beliefs
    - membership of a professional or trade association
    - membership of a trade union
    - sexual orientation or practices
    - criminal record

    that is also personal information.

- health information about an individual
- genetic information about an individual that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification or
- biometric templates.

Sensitive information is generally afforded a greater level of protection under the Privacy Act.

The type of information collected will vary depending on the purpose for collection. These purposes for collection are discussed at Section 4 – The purposes for which we collect, hold, use and disclosure your personal information. Broadly, the types of information collected includes, but is not limited to:

- name
- date of birth
- gender
- contact details such as address, email address and telephone numbers
- country of residence or citizenship
- country of birth
- ethnicity
- religion
- main language and English/reading proficiency
- passport/travel document number, country and expiry date
- visa grant details
- employment status, occupation/career history and qualifications.
- years of schooling, years of further education
- enrolment details
- family details/history
- health details
- medical reports, x-ray images
- criminal history
- personal identifiers such as fingerprint images and facial images
- copies of any identity documents
- financial details
- information for the purpose of determining age
- refugee status/background, months in refugee camp, any associated medical alert, torture/trauma issues, and protection claims
- interpreter requirements
- relationship status
- passenger name record information including flight/vessel details, port code

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- visa subclass and expiry date
- information and intelligence from other government agencies, organisations and foreign governments
- allegations
- information obtained through warrants
- foreign immigration intelligence
- surveillance reports
- interview reports from third parties
- security assessment
- care plan notes
- incidents and visitor information
- staff information including biographical details, tax file number, next of kin, information related to security clearance, staff development, training details, medical information, compensation details, salary/payment details and details of accounts with financial institutions
- information relating to our website access such as IP or server address, the date and time of the visit to the site, pages accessed, operating system, web browser version and type, time taken to transmit information to the person, previous internet address from which the person came directly to this website.

3. How we collect your personal information

We only collect personal information for purposes reasonably necessary for, or directly related to, the Department's functions or activities, pursuant to the Administrative Arrangements Orders and portfolio legislation. This includes, but is not limited to, the *Australian Citizenship Act 2007*, the *Customs Act 1901* and the *Migration Act 1958.*

Individuals have the option of dealing anonymously or by pseudonym with the Department (APP 2). However, this may not be possible where the Department is required or authorised by law or a court or tribunal order to deal with identified individuals, or it is impracticable for the Department to deal with individuals who have not identified themselves.

Our usual practice is to collect personal information directly from the individual or their authorised representative. We may collect this information through interviews, application forms and other official forms.

We often also collect personal information from other sources. These include third parties or publicly available sources. Third parties include:

- other Australian government agencies
- law enforcement agencies
- foreign governments
- sponsors
- medical practitioners
- organisations that a person has nominated
- education providers
- employers
- members of the public who contact us with information.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

If clients are concerned about the inherent risks associated with transmission of information over the internet, we can communicate with them through other avenues. Online, all interactions between clients and us are protected by an industry standard 128-bit SSL encryption technology. We employ firewall technology to help to protect our internal systems and personal information against intrusion from the internet.

We also use Qualtrics, a third party software supplier to administer online surveys. These help us improve our services. Access to survey response data is tightly controlled and restricted to nominated departmental personnel. Data collected by Qualtrics is securely collected and managed onshore in Australia. This is in accordance with their privacy statement.

You can find more information on the storage and security of the personal information we hold at Section 5 – How we hold personal information.

4. The purposes for which we collect, hold, use and disclose your personal information

We are authorised under our portfolio legislation to collect, use and disclose a range of personal information. This legislation includes, but is not limited to, the:

- *Australian Border Force Act 2015*
- *Australian Citizenship Act 2007*
- *Customs Act 1901*
- *Migration Act 1958*
- Privacy Act.

We will use or disclose personal information (including sensitive information) for the purposes for which it was collected, and for secondary purposes where permitted by law.

We frequently use personal information for a secondary purpose where reasonably necessary for enforcement-related activities conducted by or on behalf of the Department (or another enforcement body). We may also use the information in circumstances where a person would reasonably expect us to use it for a secondary purpose. This can be either directly related to the primary purpose (for sensitive information) or related to the primary purpose (for other personal information). For example, the information provided for the primary purpose of processing one visa or citizenship application can be used for the secondary purpose of subsequent applications.

Our primary purpose when collecting personal information is to carry out our functions and activities. We manage the following programs:

- visa and migration
    - including processing visa claims and migration applications
- customs and excise
- certain Australian laws including:
    - taxation
    - health
    - quarantine

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

    - commerce
    - criminal
    - intellectual property
    - community protection.
- refugee and humanitarian assistance and programmes. These include the humanitarian programme outside Australia and protection programme in Australia
- border management including:
    - facilitating the entry of genuine travellers to Australia while preventing entry of those likely to threaten Australia's national interests
    - explaining the need for identity, health, character and security checks
    - recording the arrivals and departures of travellers and goods to and from Australia (movement records)
    - facilitating the transfer and recording of goods over the Australian border.
- visa compliance and immigration status resolution including the:
    - detection and location of persons who have no lawful authority to be in Australia or people in breach of their visa condition(s)
    - cancellation or refusal of visas to non-citizens who might be of concern to the public. This could be for reasons such as involvement in serious criminal activity.
- immigration detention, removal or transfer to a regional processing country. This includes working with service providers and foreign authorities in support of offshore processing, such as law enforcement, as well as the provision of welfare services and settlement
- citizenship, including the assessment of applications

We also conduct the following administrative activities:

- processing freedom of information (FOI) requests under the *Freedom of Information Act 1982* (FOI Act), privacy requests under the Privacy Act, and administrative access requests
- staffing and personnel related activities
- complaint handling procedures, including complaints lodged with:
    - the Ombudsman's Office
    - Office of the Australian Information Commissioner (OAIC)
    - Australian Human Rights Commissioner
    - our Global Feedback Unit.
- maintaining our website.

Enforcement Related Activities and Law Enforcement Purposes

In understanding our ability to collect, use and disclose personal information under the Privacy Act, it is important to be aware that we are an enforcement body for the purposes of the Privacy Act.

As an enforcement body, we can collect, use and disclose personal information (including sensitive information) where it is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by or on behalf of us (or another enforcement body).

Enforcement related activities of the Department include (amongst others):

- detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law
- identifying and locating unlawful non-citizens and resolving their immigration status. This includes the removal of unlawful non-citizens from Australia

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- preventing and reducing illegal migration, people smuggling and trafficking in persons
- identifying and assessing claims by non-citizens for protection in Australia. This includes managing the detention or release into the community of protection claimants
- assessing and enforcing compliance with visa and citizenship requirements
- identifying and assessing prior to arrival those entitled to lawfully enter Australia
- managing the entry and departure of people crossing the Australian border
- resolving the identity, health, national security and criminal history status of people applying to enter Australia
- collecting information to assess the identity, character and criminal history of applicants for Australian citizenship
- cooperation with other agencies, including information-sharing, for law enforcement and border security purposes, and the protection of public revenue.

We are permitted to disclose personal information to law enforcement bodies (amongst others) and intelligence bodies for the purpose of enforcing the criminal law, laws imposing a pecuniary penalty or for the purpose of protecting public revenue (amongst other things). Usual disclosures include to:

- Australian and overseas law enforcement bodies to assess character issues
- Australian and overseas law enforcement bodies and intelligence agencies or commissions, National Common Police Services, Interpol, regulatory commissions, parliamentary commissions of inquiry, international tribunals and overseas immigration authorities, to identify or investigate immigration fraud, national security issues, or suspected involvement in international crimes such as war crimes, crimes against humanity or genocide
- the Australian Federal Police, under information-sharing agreements
- the Australian Taxation Office, Centrelink and other Commonwealth or State and Territory agencies, to assist the enforcement of immigration or visa conditions
- the Australian Taxation Office and Australian police forces to locate unlawful non-citizens
- the Director of Public Prosecutions prosecuting migration or citizenship offences
- foreign governments for the removal of an unlawful non-citizen or transfer to a Regional Processing Country
- registered educational institutions, employers, sponsored persons, sponsors and labour suppliers to monitor compliance with visa conditions and sponsorship obligations, and notify instances of sanctions imposition.

Additional disclosure purposes

In addition to disclosures for the primary purpose of collection and for enforcement related activities, the Department may also disclose your personal information for the following purposes, amongst others:

- to other government agencies to:
    - confirm identity
    - verify the authenticity of documents provided
    - undertake data matching
    - manage compliance obligations
    - obtain information where their portfolio legislation provides them with a power under an Australia law to obtain certain personal information
- to keep your nominated representatives informed. This could include:
    - a family member
    - a migration agent

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

    - your travel agent
    - airlines
    - Ombudsman
    - Member of Parliament
    - solicitor
- to facilitate merits or judicial review of a decision
- to assess suitability to hold a professional licence by disclosing information to licensing authorities about migration status and work
- where it is authorised by portfolio legislation including but not limited to the *Australian Border Force Act 2015*, the *Australian Citizenship Act 2007*, the *Customs Act 1901* and the *Migration Act 1958*
- where contact details may be provided to Australian law enforcement bodies or emergency services in the event of an emergency, serious injury or death
- to Centrelink to facilitate release of bonds paid or identification and recovery of debts incurred
- for employment, labour supply and business skills. This includes to employers, labour suppliers and third parties who use clients services through a labour supply arrangement. For example, when a person applies for work, we may disclose to the employer or labour supplier information about their eligibility to work. We may also disclose information to state and territory economic development departments and agencies that help business skills migrants access government business information and services
- for training and education. This includes:
    - assisting those seeking to undertake training or education in Australia
    - determining any impact of a proposed workplace component on the Australian labour market
    - to assess overseas qualifications for some classes of visas
    - to facilitate English language tuition under the Adult Migrant English Programme
    - to monitor registered training organisations
- for health purposes including:
    - to determine whether the health requirement is met for granting a visa
    - for consideration of whether the health requirement should be waived
    - for management of public health risks
- for the refugee and humanitarian entry and on-shore protection including to the United Nations High Commissioner for Refugees (UNHCR) for the purpose of verifying identity, and humanitarian or protection claims, and the International Organization for Migration to assist its delivery of services
- for detention purposes including State and Territory welfare agencies in relation to detention arrangements, care for unaccompanied minors or detainees with physical and mental health disabilities, state and territory correctional services to facilitate transfers and confirm immigration status, schools, medical practitioners and health and welfare services providers, or migration advisors providing services to detainees or assessing options to assist the detainee. We may also provide personal information concerning people in immigration detention to independent observers contracted to participate in interviews involving minors. These observers are bound by the same privacy obligations that bind us.
- for the welfare and protection of children including:
    - organising and monitoring care and welfare arrangements in immigration detention and/or in the community
    - investigating possible abuse or neglect
    - facilitating travel arrangements and documentation

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

    - information relating to children entering Australia for adoption may be disclosed to adoptive parents, prospective adoptive parents and state/territory welfare organisations responsible for inter-country adoption issues
    - with regard to children in detention, information may be disclosed to education providers to enable those children to be enrolled in school programs.
- research, evaluations and surveys including to conduct and analyse research, evaluation and surveys about the Department's programs and services, insofar as it adheres to the confidentiality and privacy clauses in our contracts, to facilitate demographic research on new arrivals and analysis of various migration programmes and settlement outcomes and to assist settlement planning or provide settlement services.
    - Our publications do not reveal information that could identify individuals. Where surveys are conducted, we will inform clients of how data will be used. Where research is conducted by a contractor, the contract will include conditions regarding the use and disclosure of information.
- administrative activities including Code of Conduct investigations and injury management

Disclosure of personal information to overseas recipients

We may need to provide your personal information to an overseas recipient as part of our work.

We use contractors to collect, transmit and store data, including providers located outside Australia.

In some circumstances personal information is disclosed to recipients outside Australia. Often the recipient will be the person's country of usual residence or the country the person has departed from (unless the person is awaiting an assessment of protection claims). This will include disclosures to airlines or travel agents in respect of advanced passenger processing and electronic visa processing.

We exchange information with countries or international organisations that have information sharing agreements with Australia. These information exchanges might involve sharing personal identifiers. If there is a match with personal identifiers, we may disclose:

- biographical data
- copies of travel and other identity documents or information from such documents
- immigration status and immigration history (which might include any immigration fraud and offences)
- any relevant criminal history information.

The purpose of such disclosure is to help confirm identity and determine if the person has presented to other agencies under the same identity and with similar claims. The Migration Act imposes limits on the disclosure of identifying information of applicants for protection visas to foreign governments in respect of which the claim is made, unless:

- the applicant has requested or agreed to return to the foreign country
- the person's application has been refused and finally determined.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

5. How we hold personal information

Personal information collected by us is held in electronic databases. Some personal information is also held in paper files.

The databases maintain audit trails whenever personal information in electronic records is accessed, added, amended or deleted on the database.

A departmental record containing personal information can only be destroyed after it has reached its destruction date as identified in a Records Authority issued by the National Archives of Australia. When no longer required, personal information is destroyed in a secure manner, in accordance with Australian Government records management regulations, guidelines and authorities, including the *Archives Act 1983*, Records Authorities and General Disposal Authorities.

Storage and data security

The Commonwealth has developed a Protective Security Policy Framework (PSPF), which includes information security management policies.

The PSPF ensures that:

- all official information is safeguarded to ensure its confidentiality, integrity, and availability by applying safeguards so that:
    - only authorised people, using approved processes, access information
    - information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements
    - information is classified and labelled as required
- all information created, stored, processed, or transmitted in or over government information and communication technology (ICT) systems is properly managed and protected throughout all phases of a system's life cycle. This is in accordance with the protocols and guidelines set out in the PSPF, which includes the Australian Government Information Security Manual, produced by the Australian Signals Directorate.

The following is a brief summary of our current practices and procedures in storing and securing data:

- access to information collected from clients is restricted to authorised persons on a need-to-know basis
- our internal networks and databases are protected using firewall, intrusion detection and other technologies
- applications made using online services and e-services sections of our website are encrypted
- paper files containing sensitive information are protected in accordance with Australian Government Security policy. They are secured in locked cabinets, Australian Government-approved security containers or Secure Rooms with restricted access
- our premises are under 24-hour surveillance. Access is via security passes only, with all access and attempted access logged electronically
- we regularly conduct system audits and staff training. This ensures we adhere to our established protective and computer security practices.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Visits to our website

We log a record of each visit to our site. We record information for statistical purposes and we use it to:

- monitor the use of the site
- discover what information is most and least accessed
- make the site more useful.

We analyse the information we collect to show broken links on our website, bottlenecks, and other site problems. We use this information to maintain the site for efficient use. We might also collect information about the IT device you use. We could use this information to identify you so we can carry out our functions and activities.

Cookies

We use cookies for maintaining contact with a user through a website session. A cookie is a small file supplied by us, and stored by the web browser software on a person's computer when they access our site. Cookies allow us to recognise people as individual web users as they browse the website.

Our website uses two cookie types - session cookies and persistent cookies.

Session cookies exist only for the duration of a web browser session with a particular website/host. These cookies will be immediately lost when a person ends their internet session or shuts down their computer. Our copy of each user's information will be automatically deleted twenty minutes after they have last used the system. We only use this information to help people use our website systems more efficiently. We do not use the information to track their movements through the internet, or to record personal information about them.

Persistent cookies stay in one of a user's browser subfolders until that person deletes them manually or their browser deletes them based on the duration period contained within the persistent cookie's file. This period is usually beyond the termination of the current session.

No personal information is stored within cookies used by our website. We will not attempt to identify anonymous users or their browsing activities unless legally compelled to do so. This may include where a law enforcement body exercises a warrant to inspect the Internet Service Provider's log files.

6. Access, correction and complaints

Data quality

We take steps to ensure that the personal information we collect is accurate, up-to-date and complete. These steps include correcting personal information, when it is reasonable to do so, that is:

- inaccurate
- out-of-date

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- incomplete
- irrelevant
- misleading.

We conduct regular audits and quality inspections to ensure the accuracy and integrity of information. We check information regularly, and promptly resolve any systemic data quality issues that we identify.

Access to personal information

Individuals can request access to information about themselves in departmental documents (other than exempt documents) under APP 12 of the *Privacy Act* or *Freedom of Information Act 1982* (FOI Act).

An individual can seek to obtain original documents or copies of personal information by completing Form 424A Request for access to documents or information. This will allow us to track and monitor each request to ensure that we meet our legislative obligations under the FOI Act or Privacy Act. We have a statutory 30 day period to respond to the request.

Corrections of personal information

Individuals can seek to amend or annotate their personal information. How we amend or annotate a record depends on a number of circumstances.

Australian citizens

Australian citizens seeking to change their personal information on their evidence of Australian citizenship such as name or date of birth should apply to Change a citizenship certificate. They will need to provide the required documents and fee in accordance with instructions on the form.

ImmiCard holders and changes under FOI and Privacy Acts

Applicants can request to change biographic details on an ImmiCard (name or date of birth) by completing an ImmiCard amendment request. Applicants will need to attach official documentary evidence and/or an Australian Government issued Change of Name or Marriage Certificate to support the requested change.

We will consider issuing a new ImmiCard with amended biographic details following assessment of the online request and the evidence provided. The request may be referred to a case manager for an identity assessment as part of the visa process.

Non Australian citizens (permanent and temporary visa holders) with supporting documentation

Where an individual has official documentation in support of an amendment or correction, such as a passport or Australian Government issued Change of Name or Marriage Certificate, they should submit their request in writing using Form 1022 - Notification of Change in Circumstance or Form 1023 - Notification of Incorrect Answers. The individual can submit the form through an ImmiAccount or send it to the nearest departmental office. They will need to include high-resolution scans (600dpi) of certified documentary evidence to support the identity change. An authorised case officer or relevant visa processing area may action the change.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Where the change is not supported by documented evidence

Where an individual's request is not supported by official documentary evidence, and a decision is made under the Privacy Act to refuse correction, the individual can apply under the FOI Act to amend or annotate their personal records. A decision to refuse amendment under the Privacy Act must include the reasons for refusal. We should advise the individual that they can complete and submit Form 424C - Request for amendment or annotation to personal records. We will then make a decision under the FOI Act. We should also advise them that obtaining documentary evidence is highly recommended.

Under the legislation that governs it, we do not have any power to 'create' a new identity. This includes where a person chooses to change their name. Under Australian law, the State and Territory Registrars of Births, Deaths and Marriages (RBDM) are the responsible authorities for preferred name changes.

Complaints

Making a complaint to us

If a person believes we have wrongly collected or handled their personal information, they can complete an online feedback form.

They can also write to:
The Manager
Global Feedback Unit
GPO Box 241
Melbourne Vic. 3001
Australia

We are committed to a quick and fair resolution of complaints. Every complaint will be investigated and complainants will be advised of the outcome.

Making a complaint to the Office of the Australian Information Commissioner

If a person is unsatisfied with our response, they can write to the Office of the Australian Information Commissioner (OAIC). The OAIC can investigate privacy complaints about the protection of personal information. They can also direct departments to change the way they handle personal information. If a person needs help lodging a compliant with the OAIC, they can call the OAIC Enquiries Line on 1300 363 992. If they are calling from outside Australia, they can call +61 2 9284 9749.

The OAIC can receive privacy complaints through:

- the online Privacy Complaint form on the OAIC's website
- by mail to:
  GPO Box 5218
  Sydney NSW 2001

  If a person has concerns about postal security, they can consider sending their complaint by registered mail.

- by fax to +61 2 6123 5145
- by email to enquiries@oaic.gov.au. Email that is not encrypted can be copied or tracked.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

A person can make a complaint directly to the OAIC rather than to us. It is likely that the OAIC would recommend that a person try to resolve the complaint directly with us in the first instance.

7. Additional information

Additional information about our privacy practices is available from the following sources:

- the Department's Privacy Notice - Form 1442i
- General information about privacy requirements is available from the Office of the Australian Information Commissioner website.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*