Australian Government
Department of Education

Complete Privacy Policy

Contents

1. Introduction

The Department of Education ('the department', 'we' or 'us') works to ensure Australians can experience the wellbeing and economic benefits that quality education provides. The department's strategic priorities include:

- ensuring quality, affordable and accessible early education and care for families
- improving schooling outcomes for children
- preparing our future workforce through globally competitive tertiary education and research sectors and
- developing a strong evidence base for effective policy that reflects and understands the varied needs of the Australian population, business and industry.

More information is available on the Department of Education website.[1]

1.1. Who should read this privacy policy?

You should read this privacy policy if you are:

- a student
- a parent or guardian
- a child care service provider
- a registered higher education provider
- a tertiary admission centre
- a principal or teacher
- an academic or researcher
- a participant in a program or service delivered by us
- a contractor, grant recipient, consultant, or supplier of goods or services to us
- an applicant for a grant or a tenderer for a contract provided by us
- a policy stakeholder who works with us
- a person whose information may be given to us by a third party, including other Australian Government agencies
- an entrant in a competition conducted by us
- a current or past employee
- a person seeking employment with us or
- any other individual whose personal information we may collect, hold, use and disclose from time to time.

[1] https://www.education.gov.au/

1.2. Purpose of this privacy policy

The purpose of this privacy policy is to:

- describe the types of personal information that we collect, hold, use and disclose
- outline our personal information handling practices
- explain our authority to collect your personal information, why it may be held by us, how it is used and how it is protected
- notify whether we are likely to disclose personal information to overseas recipients and, if possible, to whom
- provide information on how you can access your personal information, correct it if necessary and complain if you believe it has been wrongly collected or inappropriately handled.

This privacy policy has been developed to follow the 'layered policy' format, which means that it offers layers of greater or lesser detail so people can read as much as they wish and find what they need fast.

For a snapshot of our personal information handling practices, please go to the Condensed Privacy Policy.[2] This offers an easy to understand summary of:

- how we collect, use, disclose and store your personal information
- how you can contact us if you want to access or correct personal information we hold about you or complain if you believe it has been wrongly collected or inappropriately handled.

Full details of these practices are contained in this document.

There is also a supplementary document[3] that contains more detailed information about how we handle personal information relating to employment with the department and services provided to the department by contractors or labour hire workers.

1.3. *Privacy Act 1988*

The department, including its employees, contractors and agents, is subject to the *Privacy Act 1988*[4] (Cth) (the Privacy Act) and to the requirements of the Australian Privacy Principles (APPs) contained in Schedule 1 of the Privacy Act.

The APPs regulate how federal public sector agencies and certain private sector organisations can collect, hold, use and disclose personal information and how you can access and correct that information.

The APPs only apply to information about living individuals, not information about corporate entities such as businesses, firms or trusts. Detailed information and guidance about the APPs can be found on the Office of the Australian Information Commissioner[5] website.

[2] https://www.education.gov.au/using-site/privacy
[3] https://www.education.gov.au/about-us/resources/collection-personal-information-our-employment-purposes
[4] https://www.legislation.gov.au/Series/C2004A03712
[5] www.oaic.gov.au

1.4. Information covered under this privacy policy

This privacy policy has been developed in accordance with Australian Privacy Principle 1 and embodies our commitment to protecting the personal information we collect, hold, use and disclose. This commitment is reflected in our Privacy Values.

This privacy policy is not intended to cover our handling of commercially sensitive information or other information that is not defined in the Privacy Act as personal information.

'Personal information' means any information (or an opinion) about an identified individual or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.[6]

'Sensitive information' is a subset of personal information and includes information about your health, genetics, biometrics or disability, racial or ethnic origin, religious, political or philosophical beliefs, professional association or trade union memberships, sexuality or criminal record.[7] Additional requirements apply to the collection and handling of sensitive information.

2. Our personal information handling practices

2.1. Collection of personal information

Personal information may be collected directly by us, or by people or organisations acting on our behalf (e.g. contracted service providers). It may be collected directly from you, or on your behalf from a representative you have authorised.

We may also obtain personal information collected by other Australian Government agencies, state or territory governments, other third parties, or from publicly available sources. This will only occur where you consent, where it is unreasonable or impractical to collect the information only from you or where we are required or authorised to do so by law.

We are also authorised to collect personal information (which may include sensitive information) under a range of Acts that we administer, including but not limited to:

- *A New Tax System (Family Assistance) Act 1999*[8] (insofar as it relates to child care subsidy, additional child care subsidy, child care providers and child care services)
- *A New Tax System (Family Assistance) (Administration) Act 1999*[9] (insofar as it relates to child care subsidy, additional child care subsidy, child care providers and child care services)
- *Australian Education Act 2013*[10]

[6] See section 6 of the *Privacy Act 1988* (Cth) and the APP Guidelines issued by the Office of the Australian Information Commissioner.
[7] As above.
[8] www.legislation.gov.au/Series/C2004A00490
[9] www.legislation.gov.au/Series/C2004A00491
[10] www.legsislation.gov.au/Series/C2013A00067

- *Child Care Act 1972*[11]
- *Education Services for Overseas Students Act 2000*[12]
- *Higher Education Support Act 2003*[13](except to the extent administered by the Minister responsible for Indigenous Affairs and the Minister responsible for Skills and Training)
- *Student Identifiers Act 2014*[14] (insofar as it relates to higher education).

Through our Higher Education Information Management System (HEIMS), HELP IT System (HITS), and the Tertiary Collection of Student Information (TCSI) System, we also collect personal information for the Tertiary Education Quality and Standards Agency (TEQSA). We provide this information back to TEQSA for it to use for the purposes of administering the *Tertiary Education Quality and Standards Act 2011.*[15]

We will only collect information for a lawful purpose that is reasonably necessary or directly related to one or more of our functions and activities, or where otherwise required or authorised by law. For example, the department may also collect, use and disclose personal information, including sensitive information, for an 'integrity purpose' under the *Crimes Act 1914,*[16] such as the detection or investigation of misconduct or fraud,[17]or for the purposes of the *National Anti-Corruption Act 2022*.[18]

When we collect personal information, we are required under the APPs to notify you of a number of matters. These include the purposes for which we collect the information, whether the collection is required or authorised by law, and any person or body to whom we usually disclose the information, including if those persons or bodies are located overseas. We usually provide this notification by including privacy notices on our paper based forms and online portals.

2.2. Types of personal information collected by us

We collect and hold a broad range of personal information in records relating to:

- employment and personnel matters for our employees, labour hire workers and contractors (more detailed information can be found in the 'Collection of personal information for employment purposes'[19] supplementary document)
- performance of our legislative and administrative functions
- individuals participating in our funded programs and initiatives
- management of contracts and funding agreements
- management of fraud and compliance investigations, and investigations into alleged corruption or unlawful activity involving the Commonwealth
- management of audits (both internal and external)

[11] www.legislation.gov.au/Series/C1972A00121
[12] www.legislation.gov.au/Series/C2004A00757
[13] www.legsilation.gov.au/Series/C2004A01234
[14] www.legislation.gov.au/Series/C2014A00036
[15] www.legsilation.gov.au/Series/C2011A00073
[16] www.legislation.gov.au/Series/C1914A00012
[17] See subsection 3(1) of the *Crimes Act 1914* for complete definition of 'integrity purpose'.
[18] www.legislation.gov.au/Series/C2022A00088
[19] https://www.education.gov.au/about-us/resources/collection-personal-information-our-employment-purposes

- correspondence from members of the public to us and our Ministers and Parliamentary Secretaries, or correspondence otherwise referred to us by other departments or Ministers
- complaints (including privacy complaints) made and feedback provided to us
- requests made to us under the *Freedom of Information Act 1982*[20] (Cth) (FOI Act) or the Privacy Act
- the provision of legal advice by internal and external lawyers.

This personal information may include but is not limited to:

- your name, address and contact details (e.g. phone, email and fax)
- photographs, video recordings and audio recordings of you
- information about your personal circumstances (e.g. marital status, age, gender, occupation, accommodation and relevant information about your partner or children)
- information about your financial affairs (e.g. payment details, bank account details and information about business and financial interests)
- information about your identity (e.g. date of birth, country of birth, passport details, visa details, drivers licence)
- information about your employment (e.g. work history, referee comments, remuneration)
- information about your background (e.g. educational qualifications, the languages you speak and your English proficiency)
- information about your studies and training (e.g. training results, courses completed)
- government identifiers (e.g. Customer Reference Number, Tax File Number or Unique Student Identifier)
- information about assistance provided to you under our funding arrangements
- information about entitlements under Australian Government legislation.

2.3. Tax file numbers

2.3.1. Purpose of collection

A tax file number (TFN) is a unique identifier issued by the Commissioner of Taxation. The department may collect TFNs for the following purposes:

- to administer the programs we manage, including but not limited to the Higher Education Loan Programs
- to make payments of salaries and wages to eligible employees and contractors
- to administer child care financial assistance payments.

[20] www.legislation.gov.au/Series/C2004A02562

The department's collection of TFNs is authorised under the *Income Tax Assessment Act 1936* and the *Taxation Administration Act 1953*. You are not legally obliged to provide your TFN, but there may be financial consequences if you choose not to do so.

2.3.2. Prohibitions and penalties

Certain Commonwealth legislation prohibits the collection, recording, use and disclosure of TFN information. Relevantly:

A. The *Privacy (Tax File Number) Rule 2015 (TFN Rule)* and the *Taxation Administration Act 1953* (Cth) (TAA) contain prohibitions on:

(i). requiring, requesting or collecting TFN information for unauthorised purposes (TFN subrule 8(1) and subsection 8WA(1) of the TAA).

(ii). recording, using or disclosing TFN information unless permitted under taxation, personal assistance or superannuation law (TFN Rules 9 and 10; and subsection 8WB(1) of the TAA).

A breach of the TFN Rule is an interference with privacy under the Privacy Act. Individuals who consider that their TFN information has been mishandled may make a complaint to the Australian Information Commissioner. Where the breach of privacy is considered serious, the Australian Information Commissioner may seek a civil penalty.

A breach of either sections 8WA and 8WB of the TAA is punishable by a fine of 100 penalty units or 2 years imprisonment or both. *NOTE: Effective from 1 July 2017, 1 penalty unit is equal to $210. This unit value will automatically increase in line with the consumer price index from 1 July 2020 and every three years after.*

B. The *A New Tax System (Family Assistance)(Administration) Act 1999* (the Family Assistance Administration Act), *Child Care Act 1972* (the Child Care Act) and the *Social Security (Administration) Act 1999* (the Social Security Administration Act) are personal assistance laws within the definition contained in TFN subrule 6(2). These Acts contain prohibitions on the making of a record, disclosure, use, solicitation or supply of information that is protected information, which includes TFNs (sections 163 – 167 of the Family Assistance Administration Act, sections 12K, 12L, 12M, 12Q, 12R and 12S of the Child Care Act and sections 203, 204, 205 and 206 of the Social Security Administration Act). These offences are punishable by two years' imprisonment. There are exceptions permitting the collection, use or disclosure of protected information in limited circumstances, as outlined under Part 6 of the Family Assistance Administration Act, Part IIIA of the Child Care Act and Part 5, Division 3 of the Social Security Administration Act.

C. The *Higher Education Support Act 2003* (HESA) is a taxation law within the definition contained in TFN subrule 6(2). In collecting, recording, using and disclosing tax file numbers

under HESA the department, the Australian Taxation Office and higher education providers must not contravene sections 8WA and 8WB of the TAA.

2.3.3. Further information

If you would like further information about protections surrounding tax file numbers you may wish to consult:

- The Office of the Australian Information Commissioner's[21] website
- The TFN Rule which regulates the collection, storage, use, disclosure, security and disposal of TFNs. The above information is provided to comply with the department's obligation under subrule 14(1) of the TFN Rule. The TFN Rule is available on the Federal Register of Legislation[22] website
- Annex A of this Privacy Policy, which contains a table detailing prohibitions and penalties

2.4. Collection of sensitive information

In carrying out our functions and activities we may collect personal information that is sensitive information (see section 1.4 of this privacy policy). The APPs impose additional obligations on us when collecting, using or disclosing sensitive information. We may only collect sensitive information from you:

- where you provide your consent
- where required or authorised by law or
- where a permitted general situation exists such as to prevent a serious threat to safety.[23]

We also collect sensitive information where authorised to do so, for the purposes of: human resource management, preventing, detecting, investigating or dealing with corruption, misconduct and fraud, cyber-attacks against the Commonwealth, or other unlawful activity relating to the Commonwealth, and responding to inquiries by courts, tribunals and other external review bodies.

2.5. Collecting personal information from children and young people

In carrying out our functions and activities we may collect personal information about children and young people, either directly from them, through their parents or guardians, or from their education or child care providers. Where children and young people are aged 15 or over, our general policy is to collect information directly from them as they are likely to have the capacity to understand any privacy notices provided to them and to give informed consent to the collection. For children under the age of 15, or where capacity to provide consent is at issue, our policy is to notify and seek the consent of a parent or guardian, except in circumstances where seeking consent is unreasonable or

[21] www.oaic.gov.au/privacy-law/privacy-act/tax-file-numbers
[22] www.legislation.gov.au/Series/F2015L00249
[23] Permitted general situations are set out in Section 16A of the Privacy Act. (www.legislation.gov.au/Details/C2019C00025/Html/Text#_Toc534973664)
Also, see APP Guidelines – Chapter C for further information on the range of '*permitted general situations*' (https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines).

impracticable, or where the collection is required or authorised by or under an Australian law or by a court/tribunal order.

2.6. Collection of unsolicited information

Sometimes personal information is not sought by us but is delivered or sent to us by either the individual or a third party without us having requested it. This information is considered 'unsolicited'.

Where unsolicited information is received by us, we will, within a reasonable period, determine whether that information is directly related to one or more of our functions or activities. If this cannot be determined, we may, as soon as practicable and in accordance with the *Archives Act 1983*[24](Archives Act) and the Privacy Act, destroy or de-identify the information. If this can be determined we will notify you of the purpose of collection and our intended uses and disclosures according to the requirements of the APPs, unless it is impracticable or unreasonable for us to do so.

2.7. How we collect personal information

We collect your personal information through a variety of channels, which may include forms or notices, online portals, social media websites and accounts, electronic or paper correspondence and from data sharing, matching or linkage arrangements with other Australian Government and state and territory agencies, or from other third parties. In some instances, this may include incidental collection of information that you or our staff members have provided to us, through data analytics undertaken in relation to our systems.

We may also collect your personal information if you:

- communicate with us by telephone, mail, email, fax or SMS
- attend a face to face meeting or event conducted by us or by people or organisations acting on our behalf (e.g. contracted service providers)
- use our websites
- participate in a survey administered by us
- interact with us on our social media platforms.

We also monitor news and media, including social media, in the public domain.

By signing paper documents or agreeing to the terms and conditions and disclaimers for electronic documents you are consenting to the collection of any personal information you provide to us.

For further information on what information we collect online see sections 2.13 and 2.14 of this privacy policy.

[24] www.legislation.gov.au/Series/C2004A02796

2.8. Remaining anonymous or using a pseudonym

You may wish not to identify yourself or to use a different name (pseudonym) when interacting with us.

In some cases, you will be able to remain anonymous or use a pseudonym, however, there will be occasions where it will be impractical for you to remain anonymous or use a pseudonym and, where appropriate, we will advise you accordingly. For example, the department may be unable to investigate and resolve a complaint you have or complete an assessment or investigation related to compliance with its procedures or policies if you do not identify yourself.

There may also be situations where the department is required or authorised by law to deal only with an identified individual, in which case it may be necessary for you to identify yourself. For example, it would be difficult for the department to give you access to your personal information under the Privacy Act or other legislation such as the FOI Act if you did not provide enough identification to satisfy the department that the relevant personal information was related to you.

2.9. Information collected by our contractors

Under the Privacy Act, we are required to take contractual measures to ensure that contracted service providers (including subcontractors) comply with the same privacy requirements applicable to us. When the department enters into agreements with contracted service providers, it imposes contractual obligations on providers to ensure they comply with relevant privacy obligations when collecting, using, disclosing and holding personal information relating to the department's programs.

2.10. Storage and data security

2.10.1. Storage

We store personal information in a range of paper-based and electronic records. Some electronic records may be stored in the cloud, including in cloud-based systems provided by our contractors.

Storage of personal information (and the disposal of information when no longer required) is managed in accordance with the Australian Government's records management regime, including the Archives Act, records authorities, general disposal authorities and other whole of government policies or standards issued by the National Archives of Australia.

2.10.2. Data security

We take all reasonable steps to protect the personal information held in our possession against loss, unauthorised access, use, modification, disclosure or misuse.

Access to your personal information held by us is restricted to authorised persons who are departmental employees or contractors, on a need-to-know basis.

Electronic and paper records containing personal information are protected in accordance with Australian Government security policies, including the Attorney-General's Department's

Protective Security Policy Framework[25] and the Australian Signals Directorate's Information Security Manual.[26]

We conduct regular audits to ensure we adhere to these policies.

2.11. Data quality

We take all reasonable steps to ensure that the personal information we collect is accurate, up-to-date, complete, relevant and not misleading.

These steps include responding to requests to correct personal information when it is reasonable and appropriate to do so. For further information on correcting personal information see section 3 of this privacy policy.

Audits and quality inspections are also conducted from time to time to ensure the accuracy and integrity of information, and any systemic data quality issues are identified and resolved promptly.

2.12. Purposes for which information is collected, held, used and disclosed

We collect, hold, use and disclose personal information for a variety of different purposes including:

- performing our management, employment and personnel functions in relation to our staff and contractors
- performing our legislative and administrative functions
- policy development, research and evaluation
- delivering services to other Commonwealth agencies and so other Commonwealth agencies can provide services, such as ICT services, to the department
- data sharing or data integration with other Australian Government agencies, including but not limited to, data sharing or data integration with the Australian Bureau of Statistics for the Person Level Integrated Data Asset (PLIDA) (formally known as the Multi-Agency Data Integration Project) and the Data Integration Partnership for Australia
- assessing eligibility for Commonwealth financial assistance in relation to higher education students
- complaints handling
- administering requests received by us under the FOI Act or the Privacy Act
- preventing, detecting, investigating or dealing with corruption, misconduct and fraud, cyber-attacks against the Commonwealth, or other unlawful activity relating to the Commonwealth.

[25] www.protectivesecurity.gov.au/policies
[26] www.cyber.gov.au/ism

This includes participation in the Fraud Fusion Taskforce, which is a multi-agency partnership working to disrupt fraud and criminal activity, including serious and organised crime

- program management
- maintaining effective working relationships with state and territory governments, non-government education authorities and providers, universities and other relevant stakeholders
- policy advice and support to our Ministers
- contract management
- management of correspondence with the public.

We use and disclose personal information for the primary purposes for which it is collected.

We will only use your personal information for secondary purposes where we are able to do so in accordance with the Privacy Act. This may include where you have consented to this secondary purpose, or where the secondary purpose is related (or if sensitive information, directly related) to the primary purpose and you would reasonably expect us to use or disclose the information for the secondary purpose, where it is required or authorised by law or where a permitted general situation exists such as to prevent a serious threat to safety.

Likely secondary purposes for which we may use or disclose your personal information include but are not limited to:

- quality assurance, auditing, reporting, research, evaluation and analysis,
- data sharing, data integration, data matching and promotional purposes,
- in connection with measures aimed at preventing, detecting, investigating, or dealing with corruption, misconduct and fraud, cyber-attacks against the Commonwealth, or other unlawful activity relating to the Commonwealth, including participation in the Fraud Fusion Taskforce.

2.13. Our website

2.13.1. Passive collection

Your information – including personal information – is collected by a variety of software applications, services and platforms used by your device and by the department to support it to deliver services.

This type of information collection is 'passive' as the department is not collecting this information directly and it does not directly relate to the department's provision of services. Your consent for your information to be collected and shared in this way is typically obtained at the time you first use an application or service on your device.

You can opt out of some of these passive data collections, including by:

- disabling / refusing cookies
- disabling JavaScript
- opting-out of Google Analytics[27]
- disabling location services on your device.

Additional advice regarding how to protect yourself online can be found at Stay Smart Online.[28]

2.13.2. Active collection

The department directly collects some of your information – including personal information – via its website. Generally, this information is collected to enable the department to properly and efficiently carry out its functions and deliver services to you.

No attempt is made to identify you through your browsing other than in exceptional circumstances, such as an investigation into the improper use of the website.

Information may be collected by:	Type of information:	Information collected to:
Internet browser Cookies Google Analytics Social media platforms Qualtrics	Your browser type Your browser language Your server address Your location (where location services are enabled on your device) Your top level domain name (e.g. '.com', '.gov', '.au', '.uk') Date and time you accessed a page on our site Pages accessed and documents viewed on our site How our website was accessed (e.g. from a search engine, link or advertisement)	Measure the effectiveness of our content Better tailor our content to our audience
the department	Name Email address	Deliver services to you Contact you

[27] https://tools.google.com/dlpage/gaoptout
[28] http://www.cyber.gov.au/

	Phone number Education history Employment history	Identify you Subscribe you to a service or update you have requested Evaluate our programs Inform policy development

2.13.3. Links to external websites and social networking services

Our website includes links to other websites. We are not responsible for the content and privacy practices of other websites. We recommend that you examine each website's privacy policy separately.

We also use social networking services such as Facebook, Twitter, Google+, YouTube, Instagram and Yammer to talk with the public and our staff. When you talk with us using these services we may collect your personal information to communicate with you and the public.

The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies. You can access the privacy policies for these services on their websites.

2.13.4. Electronic communication

There are inherent risks associated with the transmission of information over the internet, including via email. You should be aware of this when sending personal information to us via email or via our website or social media platforms. If this is of concern to you then you may use other methods of communication with us, such as post, fax or telephone (although these also have risks associated with them).

2.14. Use of digital platforms

2.14.1. Swift Digital

We use Swift Digital to manage distribution lists and email subscription services. In order to provide these services, Swift Digital may collect personal information. The personal information collected may include your name, email address, and other details as required.

We use this personal information to personalise your content and for internal reporting, including evidence-based compliance activities. Swift Digital may also track your location, device and operating system, as well as your interaction with the email sent to you using the Swift Digital platform such as the timestamp for when you opened the email and clicked on a link contained in the email. For further information about the type of personal information Swift Digital collects, please refer to Swift Digital's Privacy Policy.[29]

[29] www.swiftdigital.com.au/privacy-policy/

Swift Digital and its hosted servers are located within Australia. Your personal information collected by Swift Digital will be stored in Australia.

2.14.2. Qualtrics

The department uses Qualtrics for online application forms, to conduct internal and external surveys, and online consultations. The department may collect personal information such as name, email address, or other personal information as part of your response.

The department uses this information for a range of purposes related to our work including to review or evaluate services, programs, processes and stakeholders' experiences, or to help with the administration of our programs.

Qualtrics does not usually have access to data collected through surveys. However, personal information may be shared with Qualtrics as part of Qualtrics providing support services to the department. For more information about how Qualtrics will handle personal information, please refer to the Qualtrics Privacy Policy.[30]

Qualtrics is an international organisation with offices based around the world, including in Australia. All data collected through the department's Qualtrics licence is contractually stored in Australia, on Cloud-based data servers approved by the Australian Signals Directorate Cloud Computing List.

2.15. Sharing of personal information with other Commonwealth agencies providing services to the department

We may share your personal information with other Commonwealth agencies that provide services to the department, in particular:

- the Service Delivery Office within the Department of Finance (Finance), which provides a range of corporate services. For more information, please refer to the Service Delivery Office[31]
- the Department of Employment and Workplace Relations (DEWR), which provides a range of ICT and other corporate services
- Services Australia, which provides ICT and administrative services for us, including the management of the Child Care Subsidy System and some parts of the TCSI system (see below for additional circumstances in which personal information may be provided to Services Australia).

[30] www.qualtrics.com/privacy-statement/
[31] www.sdo.gov.au/

2.16. Disclosure of personal information to Services Australia

If you are an employee, contractor or consultant of the department, we or Finance, may disclose your personal information to Services Australia for the purposes of managing authorised access to the Child Care Subsidy System.

If you use the Australia Government Digital Identity System to access the department's services then your personal information linked to your Digital Identity (such as your given names, last name, date of birth, or email address) may be provided to the Oversight Authority of the System, currently Services Australia, in certain circumstances. Your personal information will only be provided to the Oversight Authority to assist the Oversight Authority to perform its functions, such as if a suspected fraud or cyber security incident has been detected within the System. For more information on how the Oversight Authority handles personal information, see the Oversight Authority Privacy Policy: https://www.servicesaustralia.gov.au/digital-identity-interim-oversight-authority-privacy-notice.

2.17. Disclosure of personal information overseas

We will, on occasion, disclose personal information to overseas recipients. The situations in which we may disclose personal information overseas include:

- the publication on the internet of material which may contain personal information, such as departmental reports, submissions and other documents; photographs, video recordings and audio recordings and posts and comments on our social media platforms (where consent has been given for this or we are otherwise permitted by law to provide this information) (see below for further detail)
- the provision of personal information to overseas researchers or consultants (where consent has been given for this or we are otherwise permitted by law to provide this information)
- the provision of personal information to recipients using a web-based service where data is stored on an overseas server, for example, the department may use Mailchimp for email subscriptions (see below for further detail on this service)
- the provision of personal information to foreign governments and law enforcement agencies (in limited circumstances and where authorised by law)
- where recipients of departmental communications use an email account that stores data on an overseas server, and
- where people post and comment on our social media platforms.

We will not disclose your personal information to an overseas recipient unless one of the following applies:

- the recipient is subject to a law or binding scheme substantially similar to the APPs, including mechanisms for enforcement
- you consent to the disclosure after being expressly informed that we are not able to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information

- a permitted general situations exists (e.g. to lessen or prevent a serious threat to life, health or safety) [32]
- disclosure is required or authorised by law, or by an international agreement relating to information sharing to which Australia is a party or
- the disclosure is reasonably necessary for an enforcement related activity conducted by, or on behalf of, an enforcement body and the recipient performs similar functions.

It is not practicable to list every country to which we may provide personal information as this will vary depending on the circumstances.

2.17.1. Publishing certain material on the internet

From time to time the department publishes material on the internet (in particular our website), for example, submissions made by individuals to the department. Publication on the internet by its nature may involve disclosure to overseas recipients in any country. Where you have agreed to the department publishing material on the internet that contains your personal information, the department will not be able to take steps to ensure that a recipient located overseas does not breach the APPs in relation to that published information. As such, by agreeing to the publication, you are consenting to your personal information being accessible overseas and acknowledge that APP 8.1 contained in schedule 1 of the Privacy Act will not apply to any use of that information.

2.17.2. Mailchimp

To provide our news or information the department may use Mailchimp. Mailchimp provides online platforms that can be used to create, send, and manage emails. In providing this service, Mailchimp may collect personal information, such as distribution lists which contain email addresses, and other information relating to those email addresses. For further information about the type of personal information Mailchimp collects, please refer to Mailchimp's Privacy Policy.[33]

We may use this information to manage emails relating to the work of the department, measure email news performance and to improve the features of our website and email news service. Mailchimp may transfer this information to third parties where required to do so by law, or where such third parties process the information on Mailchimp's behalf. Mailchimp uses cookies and Web Beacons to collect information about when you visit the website, when you use the services, your browser type and version, your operating system, and other similar information.

Mailchimp is based in the United States of America (USA) and the information generated by cookies about your use of the website (including your IP address) will be transmitted to and stored by Mailchimp on servers located outside Australia.

You can opt out of our mailing list if you choose the 'unsubscribe' service provided by Mailchimp in every email, or contact the department. You can also disable or refuse cookies. However, you may

[32] Permitted general situations are set out in Section 16A of the Privacy Act. (www.legislation.gov.au/Details/C2019C00025/Html/Text#_Toc534973664)
[33] www.mailchimp.com/legal/privacy

not be able to use the services provided by Mailchimp if cookies are disabled. Should you wish to contact Mailchimp, you can find contact details on the Contact Mailchimp[34] page.

If you do not unsubscribe or contact the department to opt out of the mailing list you:

- consent to your personal information being collected, used, disclosed and stored as set out in Mailchimp's Privacy Policy[35] and agree to abide by Mailchimp's Terms of Use[36]
- understand and acknowledge that this service utilises a Mailchimp platform which is located in the USA and relevant legislation of the USA will apply. This means you will need to seek redress under the laws of the USA for any privacy breaches by Mailchimp
- understand and acknowledge that Mailchimp is not subject to the Commonwealth Privacy Act and the department will not have an obligation to take reasonable steps to ensure that Mailchimp does not breach the APPs in relation to personal information that is given to Mailchimp.

2.18. Unauthorised access, use or disclosure of personal information

We will take seriously and deal promptly with any unauthorised access, use or disclosure of personal information.

The Notifiable Data Breaches (NDB) scheme in Part IIIC of the Privacy Act, which commenced on 22 February 2018, generally requires agencies and organisations to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm to those individuals. These entities are also required to notify the Office of the Australian Information Commissioner. We comply with the NDB scheme when dealing with these types of data breaches.

The department also has regard to relevant guidance material issued by the Office of the Australian Information Commissioner, including the 'Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth),'[37] when responding to any incidents involving the unauthorised access of, use or disclosure of personal information.

3. Accessing and correcting your personal information

3.1. How to seek access to and correction of personal information

You have a right under the Privacy Act to access personal information we hold about you.

You also have a right under the Privacy Act to request corrections of any personal information that we hold about you if you think the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

[34] www.mailchimp.com/contact
[35] www.mailchimp.com/legal/privacy
[36] www.mailchimp.com/legal/terms/
[37] www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

To access or seek correction of personal information we hold about you, please contact us using the contact details set out at section 6.1 of this privacy policy.

3.2. Our access and correction process

If you request access to or correction of your personal information, we must respond to you within 30 calendar days.

While the Privacy Act requires that we give you access to or correct your personal information on request, it does set out circumstances in which we may refuse you access or decline to correct your personal information.

If we refuse to give you access or decline to correct your personal information we will provide you with a written notice which, among other things, gives our reasons for refusing your request.

It is also possible to access and correct documents held by us under the FOI Act. Further information about how to make an FOI application is available on the Freedom of Information[38] page of our website. You can also contact our FOI team at foi@education.gov.au.

For further information on requesting access to, or correction of, your personal information please read our Guide to Accessing and Correcting Personal Information[39] document on our website.

3.3. If you are unsatisfied with our response

If you are unsatisfied with our response, you may make a complaint, either directly to us (see section 5 below), or you may wish to contact:

- the Office of the Australian Information Commissioner at enquiries@oaic.gov.au or telephone 1300 363 992
- the Commonwealth Ombudsman by lodging a Complaint Form[40] online or by telephone 1300 362 072.

[38] https://www.education.gov.au/about-us/corporate-reporting/freedom-information-foi/foi-disclosure-log/how-make-freedom-information-foi-request
[39] https://www.education.gov.au/about-us/resources/department-education-guide-accessing-and-correcting-personal-information
[40] www.forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=oco-complaint-form

4. Privacy Impact Assessments

4.1. What is a Privacy Impact Assessment

A privacy impact assessment (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, minimising or eliminating that impact.

4.2. When we conduct Privacy Impact Assessments

The *Privacy (Australian Government Agencies — Governance) APP Code 2017*[41] (Privacy Code) requires us to undertake a PIA in certain instances and to maintain a register of those PIAs from 1 July 2018. In accordance with the Privacy Code, we publish a version of our PIA register[42] on our website.

5. Privacy Complaints

5.1. How to make a privacy complaint

If you think we may have breached your privacy you may contact us to make a complaint using the contact details set out at section 6.1 of this privacy policy. In order to ensure that we fully understand the nature of your complaint and the outcome you are seeking, we prefer that you make your complaint in writing.

Please be aware that it may be difficult to investigate or respond to your complaint if you provide insufficient detail. You may submit an anonymous complaint, however if you do it may not be possible for us to provide a response to you.

5.2. Our privacy complaint handling process

We are committed to quick and fair resolution of complaints and will ensure your complaint is taken seriously and investigated appropriately. You will not be victimised or suffer negative treatment if you make a complaint.

For further information about our complaint handling process please read our Privacy Complaint Handling Procedures[43] document on our website.

[41] www.legislation.gov.au/Series/F2017L01396
[42] https://www.education.gov.au/using-site/privacy
[43] https://www.education.gov.au/about-us/resources/dese-privacy-complaint-handling-procedures

5.3. If you are unsatisfied with our response

If you are not satisfied with the way we have handled your complaint in the first instance, you may contact the Office of the Australian Information Commissioner to refer your complaint for further investigation. Please note that the Information Commissioner may not investigate if you have not first brought your complaint to our attention.

Office of the Australian Information Commissioner
Telephone: 1300 363 992
Email: enquiries@oaic.gov.au
Post: GPO Box 5218
Sydney NSW 2001

6. Contact Us

6.1. General enquiries, complaints, requests for access or correction

If you wish to:

- query how your personal information is collected, held, used or disclosed by us
- ask us questions about this privacy policy
- request access to or seek correction of your personal information
- make a privacy complaint

please contact us:

By mail:

Privacy Officer
Legal
Department of Education
LOC: C50MA1
GPO Box 9880
Canberra ACT 2601

By email:
privacy@education.gov.au

By telephone:
1300 566 046 (please note this is our main number)

6.2. Availability of this privacy policy

If you wish to access this privacy policy in an alternative format (e.g. hard copy) please contact us using the contact details set out at section 6.1 above. This privacy policy will be made available free of charge.

7. Privacy Policy Updates

This privacy policy will be reviewed at least annually and updated as required.

Date policy last updated: June 2024

Annex A: Prohibitions and penalties relating to the collection, recording, use and disclosure of Tax File Numbers

Legislation	Prohibitions	Exception	Penalty
Subrule 8(1) of the *Privacy (Tax File Number) Rule 2015*	Unless an exception applies, a TFN recipient must not request or collect TFN information from individuals and TFN recipients.	The request or collection is authorised by: a. taxation law; or b. personal assistance law; or c. superannuation law. Note: These terms are defined in the *Privacy (Tax File Number) Rule 2015*.	A breach of this TFN Rule is an interference with privacy under the Privacy Act. A person who considers that their TFN information has been mishandled may make a complaint to the Australian Information Commissioner. Where the breach of privacy is very serious, the Australian Information Commissioner may seek a civil penalty. The same act may also constitute an offence under subsections 8WA(1) or 8WB(1) of the *Taxation Administration Act 1953*.
Rule 9 of the *Privacy (Tax File Number) Rule 2015*	A TFN recipient must not use or disclose a TFN or record of a TFN in that way that is inconsistent with the *Taxation Administration Act 1953* or *Privacy (Tax File Number) Rule 2015*.	The use or disclosure is permitted by the *Taxation Administration Act 1953* or *Privacy (Tax File Number) Rule 2015*.	As above

Rule 10 of the *Privacy (Tax File Number) Rule 2015*	Unless an exception applies, a TFN recipient must not use or disclose TFN information (including for matching personal information about individuals).	The TFN information is used or disclosed by TFN recipients: a. for a purpose authorised by taxation law, personal assistance law or superannuation law, or b. for the purpose of giving an individual any TFN information that the TFN recipient holds about that individual.	As above
Subsection 8WA(1) of the *Taxation Administration Act 1953*	Unless an exception applies, a person must not require or request another person to quote the other person's tax file number.	To the extent required or permitted by, or reasonably necessary in order to comply with, or in connection with exercising powers under, a taxation law, a law of the Commonwealth of a kind referred to in subsection 8WA(1AA) of the *Taxation Administration Act 1953* or paragraph 8WA(1AA)(c) of the *Taxation Administration Act 1953*.	100 penalty units or 2 years imprisonment or both.
Subsection 8WB(1) of the *Taxation Administration Act 1953*	Unless an exception applies, a person must not: a. record or maintain a record of a another person's tax file number; or b. use another person's tax file number in a manner	To the extent required or permitted by, or reasonably necessary in order to comply with, or in connection with exercising powers under, a taxation law, a law of the Commonwealth of a kind referred to in subsection 8WB(1A) of the *Taxation Administration Act 1953* or paragraph 8WB(1A)(c) of the *Taxation Administration Act 1953*.	100 penalty units or 2 years imprisonment or both.

	connecting it with the other person's identity; or divulge or communicate another person's tax file number to a third person.		
Section 163 (Offence: unauthorised access to protected information) of *A New Tax System (Family Assistance) (Administration) Act 1999* (the Family Assistance Administration Act)	Unless an exception applies, a person must not intentionally obtain information that the person knows or ought reasonably to know is protected information. Note: Protected information is defined in section 3 of the Family Assistance Administration Act, which includes TFN information obtained under the family assistance law.	To the extent authorised by sections 162, 168, 169 and 169A of the Family Assistance Administration Act, where a person may obtain, make a record of or disclose protected information for particular purposes or circumstances referred in those provisions. Note: Section 162 relates to the authorised collection, use or disclosure of protected information. Section 168 relates to the Secretary's disclosure of information when necessary in the public interest to particular persons in certain cases, which must be in accordance with the *Family Assistance (Public Interest Certificate Guidelines) Determination 2015*, as made under section 169. Section 168 also allows the Secretary to disclose protected information to the head of another Commonwealth Department or authority of the Commonwealth, or where the relevant	Imprisonment for a term not exceeding 2 years.

		individual has authorised (consented to) the disclosure. Section 169A relates to the Secretary's disclosure for purposes of the administration of the child care tax offset provided by Subdivision 61-IA of the *Income Tax Assessment Act 1997*.	
Section 164 (Offence: unauthorised use of protected information) of *A New Tax System (Family Assistance) (Administration) Act 1999*	Unless an exception applies, a person must not intentionally make a record of, disclose or otherwise make use of information that the person knows or ought reasonably to know is protected information.	To the extent authorised or required under the family assistance law, the *Social Security Act 1991*, or the *Social Security (Administration) Act 1999*; or to the extent authorised by sections 162, 168, 169 and 169A of the *Family Assistance Administration Act*, where a person may obtain, make a record of or disclose protected information for particular purposes or circumstances referred in those provisions.	Imprisonment for a term not exceeding 2 years.
Section 165 (Offence: soliciting disclosure of protected information) of *A New Tax System (Family Assistance) (Administration) Act 1999*	Unless an exception applies, a person must not solicit the disclosure of protected information from an officer (or another person), where the person knows or ought reasonably to know that the information is protected information.	To the extent authorised by sections 162, 168, 169 and 169A of the Family Assistance Administration Act, where a person may obtain, make a record of or disclose protected information for particular purposes or circumstances referred in those provisions.	Imprisonment for a term not exceeding 2 years (whether or not any protected information is actually disclosed).
Section 166 (Offence: offering to supply protected information) of *A New Tax System (Family Assistance) (Administration) Act 1999*	Unless an exception applies, a person must not offer to supply (whether to a particular person or otherwise) or hold themselves as being able to supply	To the extent authorised by sections 162, 168, 169 and 169A of the Family Assistance Administration Act, where a person may obtain, make a record of or disclose protected information for	Imprisonment for 2 years.

	information about another, knowing that the information is protected information.	particular purposes or circumstances referred in those provisions. For example, an officer acting in the performance or exercise of his or her powers, duties or functions under the family assistance law.	
Section 167 (Protection of certain documents etc. from production to court etc.) of *A New Tax System (Family Assistance) (Administration) Act 1999*	Unless an exception applies, an officer must not be required to produce any document in their possession or to disclose matter of which they had notice of to a court, tribunal, authority or person having power to require the production of documents or the answering of questions.	The production or disclosure of information is for the purposes of the family assistance law; or to the extent authorised by sections 162, 168, 169 and 169A of the Family Assistance Administration Act, where a person may obtain, make a record of or disclose protected information for particular purposes or circumstances referred in those provisions.	No specific penalty is attached to this provision, but a person who discloses information in breach of this provision where no exception allowing disclosure is applicable, may breach section 164 of the Family Assistance Administration Act and may be subject to imprisonment for a term not exceeding 2 years.