# Privacy Impact Assessment – Australian Teacher Workforce Data Strategy

**For: Australian Institute for Teaching and School Leadership**

**Date: 30 May 2019**

INFORMATION
INTEGRITY
SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

# Table of Contents

# Glossary

| Abbreviation or term | Expansion or definition |
|---|---|
| ADIA | Accredited data integration Authority |
| AESOC | Australian Education Senior Officials Committee |
| AIHW | Australian Institute of Health and Welfare |
| AIHW Act | *Australian Institute of Health and Welfare Act 1987* (Cth) |
| AITSL | Australian Institute for Teaching and School Leadership |
| APPs | Australian Privacy Principles in the Privacy Act |
| ASRG | Australian Survey Research Group |
| ATWD | Australian Teacher Workforce Data collection |
| ATWDS | Australian Teacher Workforce Data Strategy |
| De-identified | Personal information is *de-identified* if the information is no longer about an identifiable individual or an individual who is reasonably identifiable. The OAIC guidelines to the APPs advise that de-identification involves removing or altering information that identifies an individual or is reasonably likely to do so, for example by: removing personal identifiers, such as an individual's name, address, date of birth or other identifying information; and removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification. |
| DET | Australian Government Department of Education and Training |
| HEIMS | Higher Education Information Management System |
| HESDC | Higher Education Student Data Collection |
| IIS | Information Integrity Solutions Pty Ltd |
| MoU | Memorandum of Understanding |
| OAIC | Office of the Australian Information Commissioner |
| Oversight Board | ATWD Oversight Board |
| Personal Information | Personal Information is defined in the Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable and whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not' |
| PIA | Privacy Impact Assessment |
| Privacy Act | *Privacy Act 1988* (Cth) |

| Abbreviation or term | Expansion or definition | 5/29 |
|---|---|---|
| Protocols | ATWD Data Access and Reporting Protocols | |
| QILT | Quality Indicators for Learning and Teaching | |
| TRA | Teachers Regulatory Authorities – the body in each jurisdiction responsible for teacher registration | |

# 1.    Executive summary

The Australian Institute for Teaching and School Leadership (AITSL) has engaged Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) on the Australian Teacher Workforce Data (ATWD) model and implementation for 2018-19.

The ATWD is a joint project between all Australian state, territory and Commonwealth governments, and aims to build a national asset known as the ATWD collection. The ATWD will combine and connect statistical data relating to all initial teacher education students and teachers in the workforce over time. Data provided from all sources will include personal data, however, this will be used for linkage purposes only.

The Education Council approved, and is funding, the ATWD following scoping work conducted in 2016. The Council appointed an Oversight Board in 2017. Other stakeholders include:

- AITSL

- Australian Institute of Health and Welfare (AIHW), which is the Accredited Data Integration Authority (ADIA)

- The Federal Department of Education and Training (DET)

- Teacher Regulatory Authorities (TRAs), which are the bodies in each jurisdiction responsible for teacher registration.

AITSL has been working with the board and other stakeholders to implement the ATWD. Initial data collection is underway.

The PIA report provides an overview of the project and maps the personal information flows involved. It then assesses the information flows against the requirements of the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (the Privacy Act) and identifies any privacy risks or gaps, and makes some recommendations to address risks identified.

## 1.1    IIS' overall opinion

IIS was engaged to conduct a high-level analysis of the privacy risks of the ATWD project as a whole, as well as specifically considering AITSL's privacy and information handling practices in its role as the lead organisation implementing the ATWD project. As such, IIS adopted the approach of understanding the lifecycle of information in the ATWD – how the information is collected, how it is handled once it has been collected and then how it might be used.

IIS notes that the PIA is being undertaken at a point when the project is well developed and data collection has commenced. Privacy has been a key concern in project design and implementation and AITSL is now seeking this assessment to ensure nothing has been missed.

IIS considers that the ATWD model and implementation has low inherent risk for both for AITSL and the ATWD as a whole. The projects aims for a statistical data collection with a clear purpose and the design of the project's information flows (e.g. de-identification, separating identifiable data and using

AIHW as the sole data repository) minimises the privacy risks. AITSL itself hold minimal personal information, if any.

IIS found that the project largely has a strong, privacy-friendly design; it identified only a few areas where some further steps would be helpful in ensuring compliance with the APPs in the Privacy Act and privacy best practice. These are:

- APP 1 – Open and transparent management of personal information, including AITSL's privacy program, which it is currently developing, and the steps it should take to monitor privacy compliance and considering the privacy impacts of any changes

- APP 11 – security of personal information, in particular regarding the issue of data destruction.

Depending on how it is handled, the collection of personal information specifically in relation to any requests from teachers to opt-out of further survey requests could also raise issues for AITSL under APP 3 and/or APP 6.

IIS discusses these issues in Section 5.

## 1.2    Recommendations

IIS has made recommendations as follows.

### Recommendation 1 – Develop a privacy monitoring and change management plan

The Oversight Board and AITSL to develop a PIA policy, which would include criteria for when further PIAs are needed for the ATWD. The policy might draw on OAIC PIA resources.

The Oversight Board and AITSL should develop a program to monitor privacy compliance, taking account of risks, obligation in the Protocols and agreements, and the APPs.

### Recommendation 2 – Develop a process to record teacher opt-outs

Develop a process to keep track of teachers who opt-out of receiving the ATWD Teacher Survey to ensure the opt-outs are honoured.

### Recommendation 3 – Develop a data destruction policy

Develop a policy and implement data destruction or a secure archiving approach for collected information.

# 2. PIA scope and methodology

## 2.1 Scope

This PIA examines the ATWD model and implementation for 2018-19. The report aims to:

- Map personal information flows for the project

- Assess information flows against the requirements of the APPs in the Privacy Act

- Identify any other privacy risks or gaps in protection, including AITSL's internal processes

- Make recommendations to ensure privacy compliance, risk management and best practice.

In providing this report, IIS makes the following qualifications:

- The PIA considered possible security or technical issues for the solution, but it did not undertake detailed investigations or reviews of the solution's technical or security features

- IIS does not provide legal advice; rather it provides strategic privacy advice

- While the PIA takes account of the roles and information handling practices of other ATWD participants it will not be reviewing their privacy requirements or approaches.

## 2.2 Methodology

In undertaking the PIA, IIS has taken the following steps:

- Planned activities for the PIA in consultation with AITSL

- Gathered information including reviewing documentation

- Met with AITSL staff in Melbourne and by phone to understand the project and discuss privacy risks

- Analysed privacy risks, taking into account: the APPs in the Privacy Act, IIS's experience with projects of this nature

- Prepared a draft PIA report and circulated the report to AITSL for feedback.

A detailed methodology for the PIA is at Appendix A.

# 3. Project description

## 3.1 Background

The ATWD project is an initiative funded by Education Council and managed by the AITSL under the supervision of the Australian Teacher Workforce Data Oversight Board (Oversight Board).[1][2] It is a joint project between all Australian state, territory and Commonwealth governments. The project is initially funded until 2021.

The project builds on earlier projects to confirm the value of the ATWD and to identify a minimum dataset and architecture. The ATWD will combine and connect data relating to all initial teacher education students and teachers in the workforce over time. Data provided from all sources will include personal data. However this will be used for linkage purposes only.

The ATWD will provide – for the first time in Australia – a complete evidence-based representation of the entire teaching workforce across Australia. The data is intended to be used to identify and report on characteristics and supply trends in pre-service teacher education and the Australian teacher workforce.

The ATWD is now in its implementation phase; data collection, including via teacher surveys, is underway. While all jurisdictions intend to participate, Western Australia, the Australian Capital Territory and Tasmania will need legislative changes before they can provide data.

Access to the data, by AITSL and other authorised and approved users, will also commence as the data collection builds. Access will be phased and controlled with more limited access and no publication of data in 2018-2019. From 2020, access, under strict conditions, will be provided to more users.

## 3.2 Overview of the ATWD

### 3.2.1 Project participants, roles and responsibilities

The ATWD has the following participants:

- Oversight Board – responsible for overall governance of the ATWD and data management and reporting protocols

- AITSL – implements the ATWD Strategy with the AIHW and on behalf of the Oversight Board to ensure high quality data is provided in the interest of the national teaching workforce

---

[1] Education Council is one of the eight Ministerial Council's responsible to the Council of Australian Governments (COAG). The Education Council provides a forum through which strategic policy on school education, early childhood and higher education can be coordinated at the national level and through which information can be shared, and resources used collaboratively, to address issues of national significance.

[2] The Oversight Board was appointed by Education Council in 2017

- TRAs – are the state and territory bodies responsible for teacher registration in Australia. They are key participants in the ATWD, providing important workforce registration information that covers all teachers across all sectors, states and territories

- AIHW – a commonwealth agency responsible for compiling health and welfare statistics and report, and an accredited Commonwealth Data Integration Authority, has been appointed to manage the data collation, linkage, security and storage required to build the ATWD

- DET – provides data it collects about students enrolled in initial teacher education in its HESDC and from the results of the QILT survey, which students are invited to complete.

- Australian Survey Research Group (ASRG) – provides a survey tool (SurveyManager) under licence to AITSL and sends completed surveys directly to AIHW.

AITSL together with representatives from all data sources including all state and territory TRAs, DET and the AIHW, form the ATWD Technical Working Group (TWG). This group provides advice to the Oversight Board on data quality, data specifications, data harmonisation, data use and interpretation, and national consistency in data collection to inform decisions around data access and reporting.

### 3.2.2   ATDW model and operation

The ATWD model consists of primary and secondary data which will be united and linked annually from the several sources.

Primary data is the key data as it can be obtained from current data collections and linked into a cohesive data set. The primary data collections, when united, complete most of the data needed for the ATWD to meet its objectives. Primary data sources include:

- teacher registration data from the state and territory TRAs

- initial teacher education data from the Australian Government's Higher Education Student Data Collection (HESDC) and Quality Indicators for Learning (QILT) survey.

A further component of the ATWD is the collection of secondary data. Because state and territory regulatory authorities collect different primary data, there is a need to collect this data to ensure consistency across all states and territories.

Secondary data will be collected through a short voluntary survey (ATWD Teacher Survey), administered annually by AITSL through the TRAs, which teachers will be able to complete at the time of registration, or at other touch points with the TRAs. Because the survey will be tailored for each state or territory, teachers will only need to provide information that is not already collected by their regulatory authority.

All teachers will be invited as part of their registration process, to participate in the ATWD Teacher Survey annually. Different states and territories will be joining the ATWD at different times, so teachers will be invited to participate as their state or territory joins.

Data for individuals across each of these sources will be linked and harmonised to ensure the ATWD contains data that is consistent across all states and territories. The AIHW will remove all personal information before the de-identified data is incorporated into the ATWD. Individual teachers will not be identifiable in the ATWD.

The ATWD will be updated annually to provide a longitudinal database, of the highest data quality and integrity, on teacher workforce supply.

### 3.2.3 Nature of personal information involved

#### 3.2.3.1 Registration data

- Basic teacher data, including:
  - Linkage demographic information (e.g. registration number, date of birth, address)
  - Demographic information (e.g. gender, country of birth)
  - Employment information (e.g. employer details, role)
- Provided by the state and territory TRAs from their internal data sources
- De-identified by the AIHW before being incorporated into the ATWD.

#### 3.2.3.2 Initial Teacher Education data

- Comprehensive initial teacher information, including:
  - Linkage demographic information (e.g. registration number, date of birth, address)
  - Demographic information (e.g. gender, country of birth, ATAR, student identifier, regionality)
  - Program information (e.g. higher education provider, course details, student financial status (not financial information), teaching specialisation (derived from course detail information), course satisfaction, course intentions)
- Provided by DET from its HESDC and QILT data sources
- De-identified by the AIHW before being incorporated into the ATWD.

#### 3.2.3.3 ATWD Teacher Survey

- Further information to supplement the Registration data provided by the TRAs, including:
  - Demographic information (e.g. number of years as an educator, post initial teacher education qualifications)
  - Employment information (e.g. contract type and length, work hours, employer details, role)
  - Teaching information (e.g. perception of helpfulness of induction, nature of teaching position, subjects taught, career intentions)
- Provided by AITSL from the survey it will administer using the SurveyManager platform hosted by ASRG
- De-identified by the AIHW before being incorporated into the ATWD.

### 3.2.3.4 ATWD Teacher Survey operation

As noted, AITSL is responsible for the data collection via the ATWD Teacher Survey. The survey has so far been run in South Australian, the Northern Territory and NSW, and other jurisdictions will follow; once fully operational it will be run annually.

The survey has been designed to allow teachers to remain anonymous. AITSL is administratively responsible, and has, for example, engaged ASRG, but at this point it is not directly involved in the data collection.

The survey procedure is as follows:

1. Surveys are created in SurveyManager platform hosted by ASRG

2. AITSL generates batches of unique links (individual for each teacher) to the survey for each jurisdiction TRA

3. TRAs send invitations containing a unique link to each teacher and keep record of the details of each link associated with each teacher

4. ASRG sends completed surveys directly to AIHW

5. AIHW associates the survey answers to each individual teacher's record.

AITSL noted that future survey administration in Victoria and the Australian Capital Territory might require the collection of teacher registration numbers (TRN); the TRAs in these jurisdictions require teachers to register every year. As part of the annual registration process, teachers would be asked to fill in the survey after completing their registration. Once completed, the surveys would be treated in the same manner as those sent out by TRAs by email, with the exception being that AIHW would use the TRN to link the survey results to the correct individual. However, IIS understands that the TRN would be separated as personal information and would not be included in the ATWD data. Provided that the steps continue to be taken to ensure the information is handled separately and securely, this would not appear to raise any additional issues.

### 3.2.3.5 Communications with AITSL

AITSL's privacy policy notes that student teachers and teachers can contact it if they wish to have their data removed from AIHW's collection, or if they wish to opt-out of receiving further surveys. IIS understands that it is likely there will be few such requests. However, at this point processes for managing such requests and the related personal information, are yet to be worked out. See Section 5.2 below.
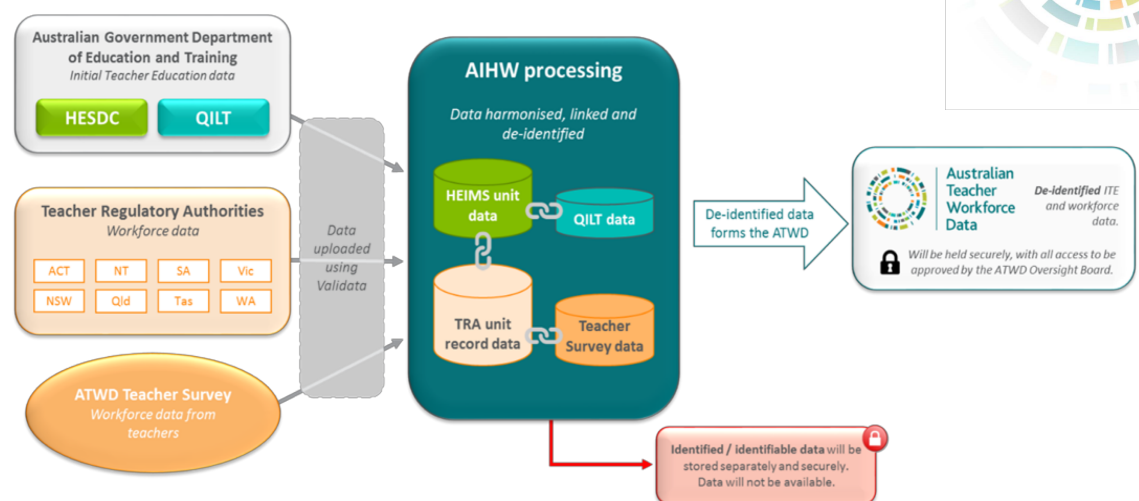
## 3.2.4   Summary of data sources

**The ATWD model at a glance**
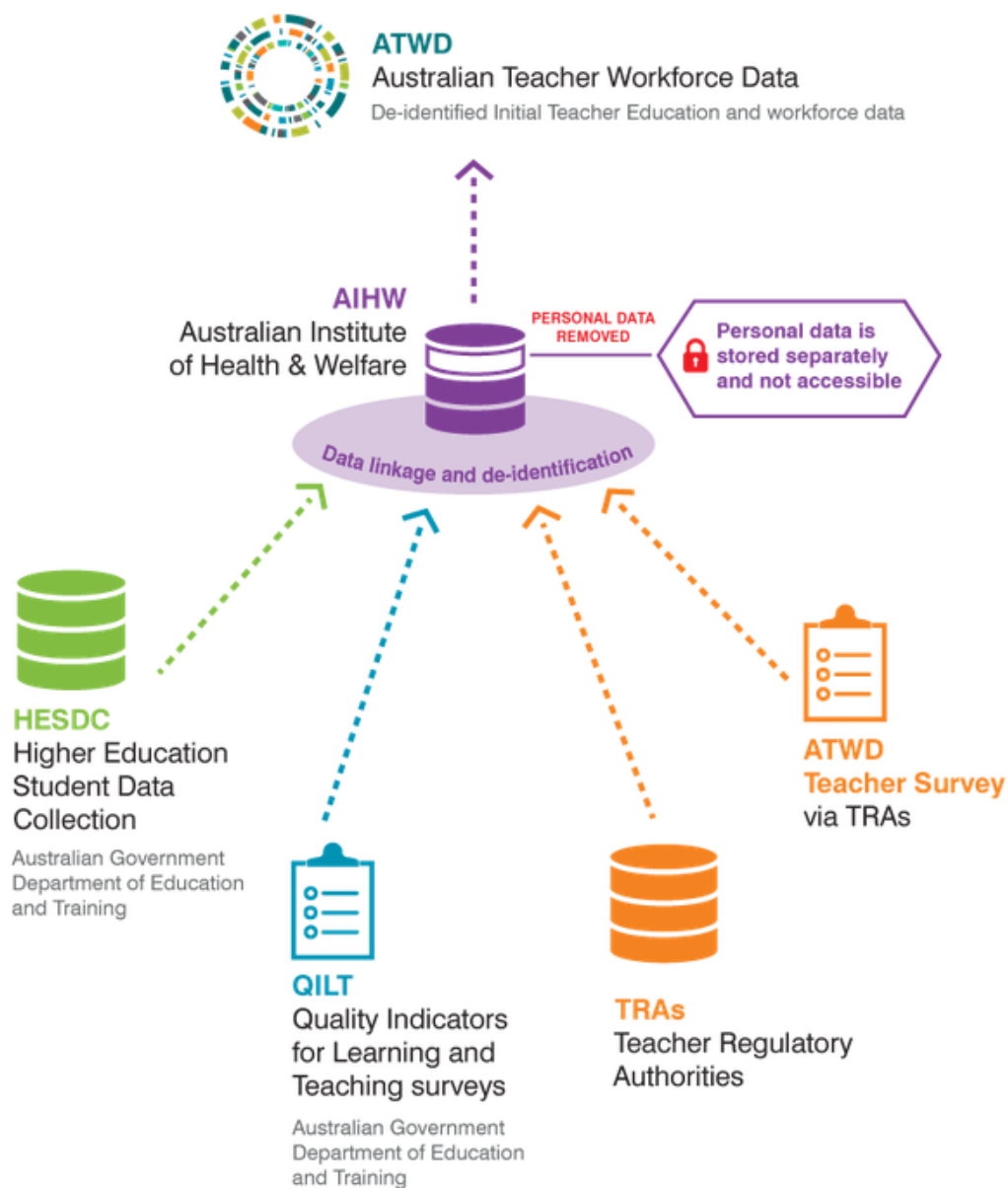
### 3.2.5   Information flows

The diagram below summarises the data flows involved in the ATWD project:



## 3.3   Project governance

The Oversight Board reports to the Australian Education Senior Officials Committee (AESOC) and is responsible for:

- 'Governance of the ATWD including management, funding accountability, privacy and risk management, and change management, to ensure current use and future use of the ATWD conforms to its intended purpose.

- Data management, access and reporting – including the set of variables, data dictionary and data specifications of the ATWD data, the NMDS, and protocols and processes for data security and privacy, data access, data analysis, data release and data interpretation and reporting.'[3]

A key element of the framework are the ATWD Data Access and Reporting Protocols (the Protocols), which govern access to and reporting of all data in the ATWD, and which set out strict guidelines for interacting with the collected data following the best practice '5 Safes Framework'.[4] The Protocols include data privacy and confidentiality provisions.

---

[3] The ATWD Data Access and Reporting Protocols, page 6

[4] The ATWD Data Access and Reporting Protocols note that the Five Safes Framework is an internationally recognised risk management methodology used widely by the Australian Bureau of Statistics, the Australian Institute of Health and Welfare and in the UK, New Zealand and Europe

Project arrangements which give effect to these provisions include:

- Formal agreements between the various stakeholders, for example between the Oversight Board and jurisdictional Education Authorities on behalf of Ministers, between AITSL and AIHW and between AIHW and the jurisdictions, setting requirements for data handling and data access and reporting, in accordance with legal requirements and the Protocols

- AITSL providing Secretariat support to the Oversight Board, including preparation of policies and procedures and risk identification and reporting

- Contract in place with ASRG, which includes privacy and confidentiality provisions

- Working groups, including the TWG.

In addition, AIHW, which has extensive experience in responsibly handling personal information, has a well-developed approach to privacy (described in its Data Governance Framework).

## 3.4 Legislative framework

AITSL is a public company limited by guarantee, established under the *Commonwealth Corporations Act 2001* and subject to the provisions of the *Public Governance, Performance and Accountability Act 2013*. It is funded by the Australian Government and the Minister for Education and Training is the sole member of the company. AITSL operates under its own constitution, with decisions made by an independent board of directors.

IIS considered the application of privacy legislation to AITSL in this context.

AITSL does not meet the agency definition as detailed in Section 6 (1) of the Privacy Act but is listed as a specified agency in Schedule 1 of Privacy Regulation 2013 and meets the agency definition under Section 5(b)(i) of Privacy Regulation 2013. Hence, AITSL is subject to the application of the Privacy Act. Although AITSL is not required to comply with the Australian Government Agencies Privacy Code it endeavours to use the code as a best practice guide.

As AIHW is a key participant in the ATWD project, the application of the *Australian Institute Of Health And Welfare Act 1987* (Cth) *(*AIHW Act) is also relevant. In particular, section 29 of the AIHW Act states that information held by AIHW is confidential. This provides protection over the information held by AIHW as part of the ATWD and also exempts the information from the reach of the *Freedom of Information Act 1982* (Cth) (FOI Act) as provided by section 45 of the FOI Act.

## 4. Approach to risk analysis

In undertaking the PIA, IIS has considered the project's inherent privacy risks. Such risks arise from:

- The nature of the personal information held, for example, its quantity, sensitivity, and potential for, and consequences of, misuse

- The kinds of people about whom the information is held, for example, their background, characteristics and vulnerabilities

- The context in which personal information is handled, for example, senior management commitment to privacy, staff privacy skills and experience, the nature of computer or other systems
- The extent to which information is accessed or handled by third parties
- The likely community and/or media interest in the privacy aspects of the project.

The inherent risk assessment considers the risks for the project as a whole.

IIS considers that the project has a low degree of risk because:

- AITSL holds some personal information in its other activities but at this point none for the ATWD project

- Whilst a significant amount of information about teachers and teaching students is being collected, the design of the project ensures only one entity (AIHW) holds all the data and it has robust de-identification processes

- Project participants are experienced and recognised – in particular, AIHW has extensive knowledge on best practice for data hosting and de-identification

- Identifiable data will be stored separately and securely and will not be made available

- The personal information collected is not proposed to be used or disclosed for any other purposes

- There is evidence of commitment to transparency, privacy notices and communication strategies

- There is evidence that privacy has been considered in project design and implementation – agreements, contracts, decisions to locate data in Australia

- AITSL has been building its own privacy capacity and has been giving this priority within the organisation

- The project has well defined benefits and is unlikely to raise community and/or media concern about the privacy aspects of the ATWD.

IIS' risk analysis took account of:

- The APPs in the Privacy Act
- Guidance from the OAIC
- Privacy by Design principles
- Privacy best practice stemming from IIS' knowledge and experience.

# 5. Analysis of privacy risks

As outlined in the PIA scope, IIS was engaged to conduct a high-level analysis of the privacy risks of the ATWD project as a whole, as well as specifically considering AITSL's privacy and information handling practices in its role as the lead organisation implementing the ATWD project.

The analysis is based on the interviews held with stakeholders and documents provided. These included, for example, the privacy notices TRAs provide to teachers, as well as AIHW's arrangements to protect the collected information. In essence, IIS adopted the approach of understanding the lifecycle of information in the ATWD – how the information is collected, how it is handled once it has been collected and then how it might be used.

A high-level assessment of the ATWD based on this approach and against the APPs is contained in Appendix B. The analysis outlines factors which affected the assessment. This includes the fact that the ATWD is now in its implementation phase – the Oversight Board, AITSL and other stakeholders have already done considerable things in getting privacy right. IIS found that the project largely has a strong, privacy-friendly design and a strong governance framework.

IIS has identified only a few area where some extra steps could be taken. These areas are discussed below.

## 5.1 APP 1 – Open and transparent management of personal information

### 5.1.1 Privacy Management Framework

APP 1 obliges APP entities to manage the personal information they hold in an open and transparent way. Specifically, APP 1.2 requires APP entities to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs and relevant privacy codes.

The steps needed will depend on the organisation's circumstances (nature of personal information held, the organisational size, structure and operating model). The Office of the Australian Information Commissioner (OAIC) provides guidance on what might be needed in its Privacy Management Framework (see Appendix C). It encourages organisations to:

- Ensure privacy culture enables compliance
- Have robust and effective privacy processes
- Evaluate and enhance privacy performance.

IIS considers that the overall ATWD project governance and implementation approach is consistent with APP 1. It includes clear governance structures, protocols for responsible information and practical actions by the various stakeholders. These include a focus on transparency about the project, comprehensive privacy notices at each point of collection and considering data location when selecting the survey provider. There are also accountability measures built in; the Oversight Board receives regular reports, including on privacy risks, and monitors, or will monitor, data access and use. In turn the Oversight Board reports to the Australian Education Senior Officials Committee of the

Education Council. The Oversight Board also plans to review the Data Access and Reporting Protocols at the end of 2019.

IIS has separately considered AITSL's privacy approach. As noted, AITSL does not currently handle personal information in the context of the ATWD. However, it has a key role in implementation and its privacy management could affect the project. While IIS considers this is sound as far as the ATWD, it understands AITSL as a whole does not yet have a formal Privacy Management Framework.

AITSL does have a clear privacy policy on its website, it has recently appointed a privacy officer and will be working to formalise its approaches.

While IIS has not identified specific ATWD project risks arising from the fact that AITSL's privacy management is still developing, a strong overall privacy environment is more likely to help minimise risks.

IIS therefore strongly supports AITSL's moves towards a more formal privacy management approach.

### 5.1.2    Monitoring privacy risks, compliance and managing change

Processes to monitor identified privacy risks as well as compliance with privacy obligations, and importantly to consider privacy when any major changes to personal information handling are contemplated, are important elements in satisfying the APP 1 requirements.

As noted, privacy and risk management, and change management, are clearly identified as part of the Oversight Board's role. The Protocol notes, for example, that the Oversight Board will 'maintain a regular process of monitoring and reviewing data access and reporting protocols and associated agreements'. AITSL will also have direct obligations under the Protocol and its agreements with AIHW will monitor compliance with these.

The processes to give effect to monitoring are being developed. AITSL asked IIS specifically about best practice from a privacy perspective, particularly with respect to conducting further PIAs.

PIAs are generally most useful when personal information practices are changing. For the ATWD, relevant changes might include new data sources, new types of access, or new uses of the data. While further PIAs might not be needed in the short term, IIS suggests it would be useful for AITSL, or the Oversight Board, to develop criteria to assess whether new activities or aspects of the project implementation would trigger the need for a PIA. The OAIC has a range of PIA resources that could provide guidance or models here.[5]

Where a project or activity is proceeding with a planned implementation or is in a business as usual phase, compliance monitoring or privacy audits or privacy health checks (which assess the extent to which an organisations' current policies, procedures and ICT platforms are compliant with the law, vulnerable to privacy risks and/or meet privacy best practice) would be better options.

---

[5] See https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

The extent of privacy monitoring/audits/privacy health checks to be undertaken and the issues to be considered will usually be a risk-based decision. Factors to be taken into account could include:

- The sensitivity and amount of personal information held

- Possible sources of privacy risk (systems, staff, expertise, processes)

- The impact on individuals, and the organisation, if things go wrong

- Stakeholder expectations, in this case, data providers, as well as the community

- Resources available.

While AITSL will not be holding much, if any, identified information, it will have a strong interest in ensuring it is permitted to access ATWD data and, to ensure continued support, that the ATWD has a sound privacy reputation. IIS suggests an appropriate program would include:

- A PIA policy that sets out when further PIAs would be needed

- Ensuring AITSL' risk framework continues to identify, assess and mitigate privacy risks

- A program of privacy compliance audits, taking account of risks, that would complement other compliance monitoring AITSL's plans for its ATWD commitments.

**Recommendation 1 – Develop a privacy monitoring and change management plan**

The Oversight Board and AITSL to develop a PIA policy, which would include criteria for when further PIAs are needed for the ATWD. The policy might draw on OAIC PIA resources.

The Oversight Board and AITSL should develop a program to monitor privacy compliance, taking account of risks, obligation in the Protocols and agreements, and the APPs.

## 5.2    APP 3 – Collection of solicited personal information and APP 6 – use and disclosure of personal information

APP 3 sets requirements including that organisations may only collect personal information where it is reasonably necessary for their functions or activities, must use fair and lawful means of collection, and, subject to exceptions, must have consent to collect sensitive information.

APP 6 requires organisation to use or disclose personal information only for the primary purpose for which is was obtained unless specified exceptions apply. These include where the use or disclosure is related to the purpose of collection and is reasonably expected.

In discussions AITSL noted that if teachers asked not to be surveyed again this request would be honoured. At this point, there is no specific option for teachers to opt-out but AITSL anticipates there could be ad-hoc requests. Also, at this point, it's not clear who would receive such requests – AITSL, ASRG or the TRAs – or how such requests would be handled. Possibly requests would need to be referred to TRAs, since they send out the emails inviting students to participate in the survey.

AITSL expects there would be few such requests. It is more likely that teachers will simply not complete the survey; for survey conducted to date there has been approximately a 20% response rate. Nevertheless IIS considers a process should be developed.

It's not completely clear at this point how the APPs, or other privacy principles, might apply. It will depend on who is actually collecting the opt-out information and how this affects further use/disclosures of teacher information in administering the survey.

Potentially, there might be issues (for some or all of the stakeholders) of fair collection or use or disclosure of information in ways that are inconsistent with privacy principles (for example because teachers were not told that their data might be used for survey) or which individuals might not expect (if they receive a survey having expressed a wish not to).

While the issue might not fit strictly within the APPs or other jurisdiction privacy principles, respecting teachers' wishes to the extent possible would be good privacy practice.

IIS therefore agrees that a procedure for handling any opt-out requests should be developed. In developing the process, AITSL should consider how to ensure it is sufficiently robust to effectively honour teacher wishes. It should also consider whether it is practical to routinely offer an opt-out to all teachers.

### Recommendation 2 – Develop a process to record teacher opt-outs

Develop a process for handling any opt-out requests. In developing the process, AITSL should consider how to ensure it is sufficiently robust to effectively honour teacher wishes. It should also consider whether it is practical to routinely offer an opt-out to all teachers.

## 5.3    APP 11 – Security and data retention

### 5.3.1    Security

APP 11.1 obliges APP entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. The OIAC has issued a guide for securing personal information.[6]

It is outside the scope of this PIA to conduct a detailed security assessment. However, as noted in its high-level risk assessment against the APPs at Appendix B, IIS considers the security approach should be sound.

APP 11.2 obliges APP entities to take reasonable steps to destroy or de-identify personal information it holds about an individual, where it no longer needs the information for any relevant purpose.

---

[6] https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

AITSL indicated that there is no policy for destroying data collected in the ATWD and no decisions have been taken on the period for data should be retained. It is expected that data would be retained for the life of the project – until mid-2021 – and if the project is extended, for a longer period.

IIS recognises that there could be sound reasons for keeping ATWD data for long periods, for example, to support the objectives in establishing the collection, and that statistical data carries less risks than identified personal information. A well-considered data destruction policy will be able to take these factors into account as well as considering any potential privacy and security risks. While not a high priority issue, IIS considers that such a policy should be on the implementation agenda, particularly if the project is extended.

### Recommendation 3 – Develop a data destruction policy

Develop a policy and implement data destruction or a secure archiving approach for collected information.

# 6.    Appendix A – Methodology

IIS took a consultative, practical and strategic approach to the consultancy and worked closely with the relevant staff of AITSL at all stages. In planning and undertaking the PIA, IIS drew on international best practice and its own depth of experience in conducting PIAs. IIS also ensured that the PIA report was consistent with the OAIC's PIA Guide. The PIA involved the following stages.

## 6.1    Planning

IIS finalised the methodology and work plan in consultation with AITSL's person. Key inputs from this phase were the legislation that IIS had to take into account and key persons to interview.

## 6.2    Information gathering and meetings

The main objective of this stage of the PIA was to ensure that IIS had a sufficient understanding of the ATWD, the nature of the personal information involved, and how it would be stored, managed and used, to inform the PIA drafting. IIS gathered information by reading relevant documents and holding meetings with AITSL's management and project team.

### 6.2.1    Documents Reviewed

| Document |
|---|
| 1.    AIHW Proposal AITSL - Implementation of the NDS |
| 2.    AITSL – AIHW MoU Teacher Survey 25 October 2018 |
| 3.    ATWDS Overview |
| 4.    ATWD Data Access and Reporting Protocols - Final |
| 5.    ATWD NMDS Data Set Specifications |
| 6.    Oversight Board sample ATWD Risk report |
| 7.    Overview Data Privacy and ATWD |
| 8.    ATWD Strategy Privacy Policy |
| 9.    Teacher Registration Board Northern Territory – privacy notices |
| 10.    AIHW Confidentiality Undertaking APS agency staff (samples) |
| 11.    ASRG – Solution and information management overview |

### 6.2.2   Meetings Held

| Meeting | Date |
|---|---|
| **Planning Kick off meeting** | 30 April |
| • Toni Mercuri | |
| • James Chong | |
| • Michael Trovato | |
| • Eugenia Caralt | |
| • Chris Cowper | |
| • Alexander Benze von Fritz | |
| **Information Gathering** | 1 May |
| • Toni Mercuri | |
| • James Chong | |
| • Eugenia Caralt | |
| • Chris Cowper | |
| • Alexander Benze von Fritz | |
| **Project update and review draft findings** | 13 May |
| • Toni Mercuri | |
| • James Chong | |
| • Chris Cowper | |
| • Alexander Benze von Fritz | |

## 6.3    Analysis

Following the information-gathering stage, IIS undertook a detailed mapping of the personal information flows and identified and analysed privacy issues taking into account the APPs in the Privacy Act as well as against broader privacy considerations.

## 6.4  Preparation of PIA report

IIS developed its recommendations and drafted the PIA report. IIS provided the draft report to AITSL and stakeholders for review and feedback. IIS finalised the report taking into account AITSL and stakeholder feedback.

# 7. Appendix B – High-level assessment of the ATWDS against the APPs

| Summary of Australian Privacy Principles | Assessment |
|---|---|
| **APP 1 — Open and transparent management of personal information**<br><br>Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy. | IIS considers that the ATWD and AITSL' privacy management approaches for the ATWD are likely to be largely consistent with APP 1. Factors in this assessment include that:<br><br>• Governance of the project is provided by the Oversight Board which will use the 5 Safes Framework to evaluate each request for access and use of the ATWD.<br>• AITSL – generally compliant with APP 1 requirements and has a clear privacy policy that details its data handling processes (although it will not be handling much, if any, personal information as part of the ATWD).<br>• AIHW – has extensive experience in responsibly handling personal information and has a well-developed approach to privacy (described in its Data Governance Framework).<br>• All participant organisations – bound by the ATWD Data Access and Reporting Protocols which set out strict guidelines for interacting with the collected data and follows the best practice '5 Safes Framework'.<br><br>IIS notes that AITSL does not have a formal privacy management framework although it has started work on this. See Section 5.1. |
| **APP 2 — Anonymity and pseudonymity**<br><br>Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply. | Not applicable for the ATWD. |
| **APP 3 — Collection of solicited personal information**<br><br>Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information. | IIS considers that the ATWD collection is generally consistent with APP 3. There are clear reasons, and benefits from the collection and there has been significant work on validating the data needed.<br><br>IIS has identified a possible issue in relation to collection where teachers seek to opt-out of future surveys, See Section 5.2. |
| **APP 4 — Dealing with unsolicited personal information**<br><br>Outlines how APP entities must deal with unsolicited personal information. | Not applicable for the ATWD. |
| **APP 5 — Notification of the collection of personal information** | No issues identified<br><br>Collection notices are presented at various times throughout the collection process and adequately address privacy matters. In particular, IIS examined a sample of the TRA privacy statements and found them to |

| Summary of Australian Privacy Principles | Assessment |
|---|---|
| Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters. | appropriately set out the information required by APP 5 – including the identity of the collecting entity and the purpose for collection.<br><br>Similarly, the collection notice presented prior to completing the survey also sets out the required information and directs users to a dedicated page hosted by AITSL regarding its data security and privacy practices (https://www.aitsl.edu.au/research/australian-teacher-workforce-data/data-security-and-privacy). This page also links to the ATWD privacy policy which provides further detailed information on the data handling and approach adopted by the ATWD project. |
| **APP 6 — Use or disclosure of personal information**<br><br>Outlines the circumstances in which an APP entity may use or disclose personal information that it holds. | No issues identified<br><br>TRAs either have legislative authority to disclose data to the ATWD or will pursue legislative amendments.<br><br>DET has authority to disclose HESDC and QILT data to the ATWD.<br><br>All data and data analysis outputs produced by users of the ATWD will be vetted by the AIHW to ensure compliance with data privacy. Authorised users are permitted to use vetted outputs of the data for internal analysis and reporting. Authorised or approved users who wish to publish outputs of the data externally, must obtain approval from the ATWD Oversight Board. |
| **APP 7 — Direct marketing**<br><br>An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. | Not applicable for the ATWD. |
| **APP 8 — Cross-border disclosure of personal information**<br><br>Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas. | Not applicable for the ATWD. |
| **APP 9 — Adoption, use or disclosure of government related identifiers**<br><br>Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual. | As set out in 3.2.3.4 above, the future administration of the survey may involve the completion of survey responses including a teacher's TRN, with this then being provided to ASRG as part of the completed survey. IIS considers that a TRN appears to meet the definition of a government related identifier. As such, ASRG could be considered to be using or disclosing the number as set out in APP 9. IIS believes it likely that this use or disclosure would be permitted by 9.2(a) of APP 9, and therefore is not a compliance issue, however this analysis should not be taken as legal advice. |
| **APP 10 — Quality of personal information**<br><br>An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also | No issues identified from a privacy perspective.<br><br>The nature and purpose of the data collection means that data quality issues, if they occur, will not have any direct impact on individuals. That said, IIS understands that the collection design considers data accuracy and has measures in place to ensure to data collection, collation and analysis processes yield accurate and reliable results. |

| Summary of Australian Privacy Principles | Assessment |
|---|---|
| take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure. | |
| **APP 11 — Security of personal information**<br><br>An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances. | The security measures to protect personal information for the ATWD appear comprehensive. These include:<br><br>• The ATWD Data Access and Reporting Protocols applicable to all participant organisations set out strict guidelines for accessing and interacting with the collected data and follow the best practice '5 Safes Framework'. The Protocols appear to comprehensively govern information security practices of participant organisations. Important security considerations such as access restrictions and data warehousing appear to be adequately addressed, with AIHW having the ability to control access to the collected data on a granular basis with sophisticated authentication protocols. In addition, access can only be granted with permission from the Oversight Board.<br>• ASRG has security provisions in place that appear to adequately protect information collected through the SurveyManager platform.<br>• AIHW has extensive experience with de-identification of data (however, IIS notes that privacy risks would emerge if de-identification is not done properly).<br>• AIHW separately and securely stores any identifiable data. In addition, section 29 of the AIHW Act specifically imposes on recipients of identifiable data released by AIHW (where this is expressly permitted by s. 29(2), for example, with the approval of the AIHW Ethics Committee), the same confidentiality obligations as those that apply to AIHW staff.<br>• AIHW states that it has a number of internal policies on Information Security and Privacy Policy and Procedures, and Guidelines for the Custody of AIHW data that impose a range of requirements. It will be monitoring adherence to the requirements.<br>• A gap identified is that there is not yet a policy in place for destroying data collected in the ATWD – this issue is discussed at Section 5.3. |
| **APP 12 — Access to personal information**<br><br>Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies. | As noted earlier, AITSL will hold limited, if any, personal information in the context of the ATWD.<br><br>AIHW will be the main participant in the ATWD to hold personal information.<br><br>Section 29 of the AIHW Act provides that information held by AIHW is confidential and must not be disclosed. As such, the information held by AIHW as part of the ATWD is exempt from disclosure under the *Freedom of Information Act 1982* (Cth) and consequently falls under the exemption to APP 12 given in 12.2(b)(i).<br><br>Although AIWH is not required to give access, AITSL has indicated that if a teacher makes a request to have their survey response deleted, AIHW would be able to perform the deletion provided the data had not already been processed and included in reports. |

| Summary of Australian Privacy Principles | Assessment | 27/29 |
|---|---|---|
| | IIS supports this approach. | |
| **APP 13 — Correction of personal information**<br><br>Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals. | No issues identified for the ATWD<br><br>As with APP 12, there are no avenues for data subjects to correct information the AIHW holds, other than requesting AITSL to delete their data. In addition, the project draws primarily on information provided by third parties and individuals concerned about data accuracy would be dealing with these issues upstream at the point of collection, for example, by jurisdictions. | |

# Appendix C – Summary of OAIC's privacy management framework

The OAIC's Privacy management framework describes steps to ensure compliance with the APPs. [7] In summary, the OAIC encourages organisations to:

- Embed a culture, and governance structure that enables privacy compliance

- Establish robust privacy practices procedures and systems, including by:

  o Keeping information about the business's personal information holdings (including the type of information held and where held (including information held off-shore or by a third party) up to date

  o Developing and maintaining processes to ensure personal information is handled in accordance with privacy obligations. Ensure these processes:

    – Address the handling of information throughout the information lifecycle (collection, storage, use and disclosure etc) giving additional consideration to areas assessed as having greater risk

    – Clearly outline how staff are expected to handle personal information in their everyday duties. Tailor these processes to align with the different needs of different areas

  o Promoting privacy awareness within your entity by integrating privacy into your induction and regular staff training programs

  o Developing and implementing a clearly expressed and up-to-date privacy policy

  o Implementing risk management processes that allow you to identify, assess and manage privacy risks across your business, including personal information security risks

  o Undertaking PIAs or business projects or decisions that involve new or changed personal information handling practices (including implementing new technologies)

  o Having processes for receiving and responding to privacy enquiries and complaints.

  o Having processes that allow individuals to promptly and easily access and correct their personal information

  o Developing a data breach response plan

- Evaluate privacy practices, procedures and systems to ensure continued effectiveness

Enhance response to privacy issues with proactive, forward thinking and anticipation of future challenges.

---

[7] Privacy management framework: enabling compliance and encouraging good practice.

**Information Integrity Solutions Pty Ltd**
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898

INFORMATION
INTEGRITY
SOLUTIONS