Maddocks

Lawyers
Level 1
40 Macquarie Street
Barton ACT 2600 Australia

Telephone 61 2 6120 4800
Facsimile 61 2 6230 1479

info@maddocks.com.au
www.maddocks.com.au

Department of Education and Training

2018 Student Residential Address Collection: Additional required information

Privacy Impact Assessment

14 September 2018

Interstate offices
Melbourne Sydney

Affiliated offices around the world through the Advoc network - www.advoc.com

Contents

Executive Summary

1. PIA Overview

1.1 In 2018, the Department of Education and Training (**Department**) will again be conducting its Student Residential Address Collection (**Project**). The Department undertakes this Project approximately every 4 to 5 years. Through the Project the Department collects a range of personal and non-personal information relating to students in non-government schools across Australia (approximately 2600 schools).

1.2 The primary purpose of the Project is to allow the Department to calculate the socio--economic status (**SES**) scores for each non-government school. The SES scores inform the funding provided by the Commonwealth to non-government schools; the scores are an indication of the anticipated capacity of a school community to contribute financially to the running costs of their school.

1.3 This year, in addition to information which has been collected from schools in previous years, the Department also intends to collect additional Personal Information (**Additional Information**) as part of the Project, to inform development of a potential new SES score methodology, which has been recommended by the National School Resourcing Board.

1.4 The Department intends that, before the collection of the Additional Information, an amendment to the *Australian Education Regulation 2013* (Cth) (**Regulation**) will be made, which will expressly authorise the Minister to request an approved authority for a school to provide the Additional Information[1].

1.5 The Department has commissioned this Privacy Impact Assessment (**PIA**) to determine whether the collection of the Additional Information as part of the Project is likely to result in the Department contravening the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**) and, if non-compliance can be avoided, minimised or mitigated, what steps the Department should take.

1.6 This PIA:

(a) assesses the risks to individual privacy presented by the collection of the Additional Information, from the perspective of the Department;

(b) considers compliance with the Privacy Act, including the APPs;

(c) may serve to inform stakeholders about the Department's commitment to consideration of privacy risks and associated risk mitigation strategies;

(d) sets out the information flows which help to highlight privacy risks and areas for improvement in terms of risk mitigation; and

(e) considers the safeguards that the Department has in place to secure the Additional Information from misuse, interference or loss, or from unauthorised access, modification or disclosure.

[1] As at the date of this PIA, the form of the proposed amendment is still being settled, but the intention is to add a new section in the Regulation (currently proposed to be section 58B) which will expressly require schools to provide certain information, including the residential address and name of each person responsible for a student.

1.7 This PIA only considers:

(a) the proposed new collection, use, and disclosure of the Additional Information – not the other types of information which has previously been collected by the Department as part of the Project for many years; and

1.7.1 the handling of the Additional Information by the Department – not handling by any other entity (including by the Australian Bureau of Statistics (**ABS**) as part of the Multi-Agency Data Integration Project (**MADIP**), which has been the subject of a separate privacy impact assessment; see paragraph 4.6 below for further details).

1.8 This PIA has been developed in accordance with the Office of the Australian Information Commissioner's (**OAIC**) *Guide to undertaking privacy impact assessments* (**PIA Guide**), and is intended to help the Department to manage privacy risks that may arise in relation to the Project.

1.9 The OAIC's *Australian Privacy Principles guidelines* (**APP Guidelines**) outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing the Department's compliance with the Privacy Act and the APPs. The analysis set out in this PIA is consistent with the APP Guidelines.

2. Summary of Findings

2.1 Maddocks has identified certain minor privacy risks related to the handling of the Additional Information, associated with the following elements:

(a) the privacy collection notice, which the Department proposes be used in connection with the Project (**Project Collection Notice**), does not contain all of the 'APP 5 matters'; and

(b) the Project Collection Notice does not expressly advise individuals that their Personal Information may be disclosed to the Department's service providers (including the Department of Jobs and Small Business as part of the provision of information and communications technology (**ICT**) support services in respect of the Project).

2.2 However, Maddocks believes that these risks may be avoided or mitigated by the Department following the recommendations set out in paragraph 3 below.

3. Recommendations

3.1 This PIA makes the following recommendations.

Recommendation 1: Amendment of the Project Collection Notice	
The Department amend the Project Collection Notice to ensure that it includes all of the 'APP 5 matters'. The Department amend the Project Collection Notice to ensure that it expressly notes that the Department may disclose Personal Information to its service providers (including the Department of Jobs and Small Business as part of the provision of ICT support services for the Project). To assist, we have included an amended Project Collection Notice at Attachment 2.	
Department response:	Accepted. The Department has amended the Project Collection Notice to incorporate Maddocks' recommended changes. The Department will use the amended version, for consultation with stakeholders. Please note there may be further changes to the notice subject to stakeholder consultations. However, in undertaking any changes the Department will ensure APP 5 matters are addressed.

Recommendation 2: Regular review	
There is a risk that over time the way in which the Department collects, discloses and uses Additional Information may change. We recommend that the Department consider whether periodic reviews should be undertaken to ensure, for example, that function creep does not occur, which gives rise to additional privacy risks.	
Department response:	Accepted. The Department supports periodic reviews of this PIA during the life of the Project; and during the development of a potential new SES score methodology to assess any additional privacy risks resulting from the collection, disclosure and use of the Additional Information.

Project Description

4. Overview of the Proposed 2018 Student Residential Address Collection

4.1 The Department collects a range of information, including Personal Information, about students in non-government schools across Australia (approximately 2600 schools) as part of the Project. This generally occurs every 4 to 5 years, following the ABS' Census of Population and Housing (**Census**). The purpose of the Project is to collect the data that will be used to calculate the SES scores for each non-government school. The SES scores inform the funding provided by the Commonwealth to non-government schools and are an indication of the anticipated capacity of a relevant school community to contribute financially to the running costs of their school. The data is also used for the purpose of policy analysis.

4.2 In previous years, the information collected through the Project has been used in conjunction with publicly available ABS Census data at the Statistical Area 1 (**SA1**) level to calculate the SES scores. Information previously collected under the Project for each student is:

(a) their School's AGEID (a reference number assigned to the school by the Department);

(b) their campus number (a reference number assigned to the school by the Department);

(c) their student reference number (a reference number assigned to the student by the school for the purpose of the collection, i.e. it is not a number used by the school to identify the student as part of its day to day operations);

(d) their residential address;

(e) whether they are a primary or secondary student; and

(f) whether they are a boarding or day student.

4.3 Subject to Government approval and appropriate regulatory amendments referred to in paragraph 1.4, from 2018 the Department will also collect the Additional Information, being the names and addresses of the parents/guardians responsible for each student as part of the Project, in addition to the information listed in paragraph 4.2.

4.4 The purpose of collecting the Additional Information is to allow the Department to:

(a) undertake analysis to support the development of a potential new SES score methodology, as recommended by the National School Resourcing Board; and

(b) assist with other policy development.

4.5 In order to do this, it is anticipated the Additional Information will be provided to the ABS, linked to other data and then de-identified by the ABS, as part of the MADIP. The key objectives of the MADIP are:

(a) to formalise data sharing arrangements for research and statistical purposes;

(b) to create a safe and secure environment for research that requires the integration of data from multiple sources; and

(c) to create an effective governance framework for data sharing.

4.6 Consideration of the MADIP is outside of the scope of this PIA. The ABS commissioned an independent privacy impact assessment in relation to the MADIP (**MADIP PIA**), and this report is available at: http://www.abs.gov.au/websitedbs/D3310114.nsf/4a256353001af3ed4b2562bb00121564/9099c77cb979d558ca258198001b27a0/$FILE/MADIP%20iPIA_2018.002.pdf/MADIP%20iPIA_2018.pdf.

4.7 After de-identification of the linked data by the ABS, the Department will use the de-identified data for the purposes set out in paragraph 4.4.

4.8 The following non-government schools are generally exempt from the Project:

(a) non-government special schools;

(b) non-government special assistance schools;

(c) non-government sole provider schools (i.e. schools operating in isolated locations where no other government or non-government school is operating); and

(d) non-government schools where the majority of students are Aboriginal or Torres Strait Islander.

4.9 Overseas students are not included in the Project as they are not funded under the *Australian Education Act 2013* (Cth) (**Act**). Similarly, distance education students are not included in the Project as under the Act they are funded at 35 percent of the base Schooling Resource Standard and the capacity to contribute assessment does not apply.

5. Collection of Additional Information

5.1 **Information collected**

5.2 As part of the Project the Department will collect the following types of Additional Information:

(a) names of the parents/guardians of each student in all applicable non-government school; and

(b) residential addresses of the parents/guardians of each student in all applicable non-government school.

5.3 This Additional Information will be Personal Information because it is about an individual whose identity is apparent, or can reasonably be ascertained from that information, and therefore meets the definition of 'personal information' in the Privacy Act. However, the Additional Information is not 'sensitive information' as defined in the Privacy Act.

5.4 The collection of the Additional Information in the Project will be expressly authorised under the Regulation (if the Regulation is amended as proposed in paragraph 1.4).

How the Additional Information will be Collected

5.5 The Additional Information will be provided to the Department by, or on behalf of, the accountable authority for each non-government school, through the School Entry Point (**SEP**) portal.

5.6 The Department only requires the school to provide information that it has already collected in relation to its students, or to make all reasonable efforts to collect the information if it does not already hold it.

5.7 Approved authorities are required to complete on online declaration in the SEP portal to verify the data.. While the Department does not require schools to verify the accuracy of the information already collected, schools are made aware that they are required to provide the information in accordance with the applicable legislation to determine funding, and that the school may be subject to an audit to confirm the accuracy of the submitted information.

5.8 The SEP portal is a Departmental web portal used by schools to provide information to the Department, including from a variety of websites related to schools funding (such as the SES website, Financial Questionnaire, Financial Accountability, Student Attendance and Non-Government School Census websites).

5.9 The SEP portal, and all data collected through the SEP portal, is stored in Australia using infrastructure owned and maintained by the Department of Jobs and Small Business. Although the level of access will differ between approved Project staff, the SEP portal is accessible by:

(a) the Department's Schools Information Technology (**IT**) staff, who oversee and maintain the SEP portal;

(b) the Department's SES helpdesk team, including contracted, temporary, and non-ongoing team members who will assist with the Project;

(c) the Department's Recurrent Assistance for Schools (**RAS**) team;

(d) approved representatives of non-government schools who are responsible for uploading the Project information into the SEP portal; and

(e) auditors contracted by the Department, in the event that the Additional Information needs to be verified for compliance purposes.

5.10 A user from the school will be able to either input the Additional Information using the Department's spreadsheet template in order to upload multiple students' details at once, or will be able to manually enter information for each individual student directly into the SEP portal. The school can use its own systems and tools to populate a spreadsheet before uploading it to the SEP portal.

5.11 Once the school has entered the relevant information into the SEP portal, the Department's ICT system automatically checks the formatting of the spreadsheets (e.g. to confirm that the school has completed all of the relevant columns and these are formatted correctly). If the system notices an issue with the formatting of a spreadsheet, it notifies the user that they must rectify the issue before being able to submit the data.

5.12 The Department's ICT system also uses Geocoded National Address File (**G-NAF**) software to validate the geographical locations entered as addresses in the spreadsheet(s). If G-NAF validates all of the addresses, the user may submit the data. If the G-NAF identifies that it cannot find an address, it notifies the user, who can then use a number of processes (including 'pinning' on a map) to identify the correct address. The Department has the ability to assist schools with this task, including through provision of a telephone helpline. The school may, if 5% or less of the addresses are not validated, still submit their spreadsheet(s).

5.13 The user is required to complete a check box declaration that all data is true and correct before they can submit the data. An approved signatory for the approved authority for the relevant school must confirm that the submitted data is true and correct. If the approved signatory is the user submitting the spreadsheet(s), no further action is needed. However, if the submitting user is not an approved signatory (that is, the user log in details do not match those for the approved signatory for the applicable approved authority), the SEP portal notifies the approved signatory that they must log in and also declare that the information is true and correct, before submission is completed.

5.14 The submitted information in the SEP portal is 'locked' when the online declaration is completed by an approved signatory for the school. If a school needs to make any changes to the submitted information after this time, an approved signatory can request that the Department 'unlock' it by emailing the SES helpdesk with the following information:

(a) the school's AGEID number;

(b) the reason why the school needs the addresses to be 'unlocked';

(c) the approved signatory's contact details, so that the Department can verify the request.

The Department will contact the school when the information has been 'unlocked', and the school can then change that information. A new online declaration needs to be made after the school has made the changes.

What individuals are told at the point of collection

5.15 The Department will not be directly involved in the original collection of the Additional Information from the individual student or parent.

5.16 The Department notifies schools that they are required to give the parent/guardian of a relevant student a Project Collection Notice titled *'2018 Residential Address Collection Notice'*. The school is given discretion to distribute the Project Collection Notice in the manner that they consider most appropriate.

5.17 The Department requires schools to declare that *'A Statement of Address Notice has been provided to the parent or legal guardian of each student for whom a residential address has been submitted',* before submission of data through the SEP portal.

6. How the Department will use the Additional Information collected

Regulatory Framework

6.1 Section 125(1) of the Act provides:

(1) The Minister may:
- (a) use or disclose school education information (including school education information that is personal information) in accordance with the regulations; and
- (b) impose conditions on any use or disclosure of school education information.

Note: This section constitutes an authorisation for the purposes of other laws, such as the Privacy Act 1988.

6.2 Section 65(1) of the Regulation reads:

(1) For paragraph 125(1)(a) of the Act, the Minister may use or disclose school education information for the following purposes:
- (a) the purposes of the Act or this regulation;
- (aa) the National School Resourcing Board;
- (b) programs administered by the Minister;
- (c) research into matters of relevance to the Department;
- (d) statistical analysis of matters of relevance to the Department;
- (e) policy development;
- (f) any other purpose determined by the Minister under subsection (3).

Note: For National School Resourcing Board, see section 128 of the Act.

(2) The Minister may also disclose school education information to the following persons for the following purposes:
(a) ACARA for the purposes of its functions;
(b) Australian Bureau of Statistics for the purposes of its functions;
(c) the Productivity Commission for the purposes of its functions;
(ca) a State or Territory body responsible for school education in the State or Territory, for the purposes of its functions;
(d) any other person determined by the Minister under subsection (3) for the purposes determined by the Minister.

Access to the Additional Information

6.3 Additional Information submitted through the SEP portal in connection with the Project will only be accessed by personnel who have been duly authorised by the Department. This may include specific authorised personnel from the teams set out in paragraph 5.9.

How the Additional Information will be used

Quality assurance process

6.4 After submission of the Additional Information (and the other information collected as part of the Project), the Department will undertake a quality assurance process. The Department will use information which was previously collected by the Department about the school to check that there are no obvious anomalies in the submitted data (including the Additional Information). The previously collected information comprises aggregated data only, and does not contain any Personal Information.

Use of Additional Information for MADIP project

6.5 The Department will use the Additional Information for the purposes of an approved project under the MADIP.

6.6 MADIP is a partnership among six Australian Government agencies that brings important national datasets together securely to maximise their value for policy analysis, research, and statistical purposes. The participating agencies are the ABS, the Australian Taxation Office, and the Departments of Education and Training, Health, Human Services, and Social Services.

6.7 Each agency participating in the MADIP collects Personal Information related to its functions or activities, and discloses this information to the ABS for the MADIP as authorised by law for policy analysis, research, and statistical purposes. The ABS conducts the MADIP in accordance with its functions to collect, compile, analyse, and disseminate statistics established by the *Australian Bureau of Statistics Act 1975* (Cth) and the *Census and Statistics Act 1905* (Cth).

6.8 The Department will disclose the Additional Information to the ABS for the MADIP, by providing the raw data to the ABS by uploading it to an ABS Secure Deposit Box, which is a mechanism for lodging statistical files or text to the appropriate ABS collection area via a secure link. Each file that is lodged is encrypted during transmission to the Secure Deposit Box and is immediately moved into a secure location where its content is automatically scanned for viruses.

6.9 The Department is satisfied that the ABS has sufficient security and data protections in place in relation to the transmission and storage of the Additional Information to and by the ABS.

Future use of the Additional Information

6.10 The Additional Information which is collected constitutes a Commonwealth record and the retention and destruction of this information is governed by the *Archives Act 1983*.

6.11 In future years, the Department may use the Additional Information in order to inform future SES scores and for further policy development.

7. Disclosure of Additional Information outside of the Department

7.1 As discussed above, the Department will disclose the Additional Information to the ABS, in the form of raw data, for an approved MADIP project for policy analysis, research, and statistical purposes.

7.2 The ABS, as the accredited data integrating authority under MADIP, will then link the Additional Information with other Personal Information. The ABS will then de-identify the data by removing individual identifiers, and make the de-identified data available in the ABS' secure DataLab for MADIP. Details of procedures and other protections that the ABS has put in place to handle the data on behalf of the MADIP partners are described within the MADIP PIA (but consideration of these is out of scope for this PIA).

7.3 The Department will only be able to access the de-identified information in the ABS DataLab through its personnel who have been seconded to the ABS to work on this MADIP project. Departmental personnel who have access to the DataLab will be subject to the same rigorous security, privacy, and confidentiality requirements as ABS staff, including strict confidentiality requirements imposed by the *Census and Statistics Act 1905* (Cth).

7.4 The Department will receive de-identified data from the ABS in the form of a confidentialised unit record. This is data which not only has had individual identifiers removed, but has also been further treated by the ABS to reduce as far as possible the likelihood that any individual may still be reasonably identified from the data set. Accordingly, the confidentialised unit record is not 'personal information' for the purposes of the Privacy Act.

7.5 The Department will use the de-identified outputs received from the ABS for various policy analysis, trend identification and policy development purposes. This may include development of a new methodology for calculating SES scores.

7.6 The Department has no plans to use the de-identified outputs received from the ABS in any manner involving further linkage with other data sets, which might result in the possible re-identification of any individual.

7.7 As mentioned in paragraph 5.9, the Department may also disclose (through provision of potential access for support and maintenance activities) the Additional Information to its ICT service providers, and may disclose the Additional Information to contracted external auditors engaged by the Department to assist with compliance activities.

Analysis

8. Personal Information Flows

8.1 Key collections, uses, and disclosures of Additional Information relevant to the Project, from the perspective of analysing privacy impacts are described below.

8.2 The Department will **collect** Additional Information (which is Personal Information about an individual) when the relevant school submits the data through the SEP portal to the Department that contains information about the individual.

8.3 The Department will **use** the Additional Information in the Project to:

(a) provide the information to the ABS for an approved MADIP project, to generate de-identified statistical data; and

(b) assist with policy development.

8.4 The Department may **disclose** Additional Information in the Project to:

(a) the ABS;

(b) its ICT service providers (engaged by the Department of Jobs and Small Business, through an MOU with the Department for the provision of ICT support services), through the potential provision of access to the SEP portal for support and maintenance purposes; and

(c) contracted auditors, who may be asked to verify the veracity of the Additional Information provided by a relevant non-government school.

9. Assessment of compliance with the APPs

9.1 Each collection, use and disclosure of Personal Information relating to the Project must be assessed against the APPs. A detailed analysis is set out at **Attachment 1**. A summary of the assessment against each APP is provided below.

9.2 **APP 1:** The Department is taking reasonable steps in relation to the management of the Additional Information, as required under APP 1.

9.3 **APP 2:** The collection, use and disclosure of Additional Information as part of the Project complies with APP 2.

9.4 **APP 3**: The collection, use and disclosure of Additional Information as part of the Project complies with APP 3.

9.5 **APP 4:** Nothing in relation to the collection, use and disclosure of Additional Information as part of Project would prevent the Department from complying with APP 4.

9.6 **APP 5:** The Project Collection Notice does not contain all of the required 'APP 5 matters'. We **recommend** that the Department update the Project Collection Notice to include all of the 'APP 5 matters'. We have included an amended Project Collection Notice at Attachment 2.

9.7 **APP 6**: The collection, use and disclosure of Additional Information as part of the Project complies with APP 6. However, we **recommend** that the Project Collection Notice expressly provide that the Department may disclose Personal Information to its service providers (including the Department of Jobs and Small Business for the purpose of the provision of ICT support services relating to the Project and external contracted auditors).

9.8 We also **recommend** that the Department considering undertaking regular reviews of the Project to ensure that function creep does not occur.

9.9 **APP 7:** APP 7 is not relevant for the purposes of this PIA.

9.10 **APP 8:** The collection, use and disclosure of Additional Information as part of the Project complies with APP 8.

9.11 **APP 9:** APP 9 is not relevant for the purposes of this PIA.

9.12 **APP 10:** The collection, use and disclosure of Additional Information as part of the Project complies with APP 10.

9.13 **APP 11:** The collection, use and disclosure of Additional Information as part of the Project complies with APP 11.

9.14 **APP 12:** Nothing in relation to the collection, use and disclosure of Additional Information as part of the Project would prevent the Department complying with APP 12.

9.15 **APP 13:** Nothing in relation to the collection, use and disclosure of Additional Information as part of the Project would prevent the Department complying with APP 13.

10. Assumptions

10.1 Maddocks has prepared this PIA in consultation with the Department. Maddocks has relied on the Department for the description of the Project, and has drafted the PIA on the assumption that the description of the Project accurately reflects how the Department will handle the Additional Information.

10.2 This PIA does not:

(a) provide an analysis of compliance by the Department of any statutory secrecy provisions that may be applicable to it (no secrecy related issues have been identified by the Department in respect of legislation it administers); or

(b) consider the terms of any privacy policies of the Department, or of any service providers, or their compliance with those policies; or

(c) consider privacy issues associated with the handling of the Additional Information by the ABS (or any other entity to which the Additional Information is disclosed), or any information collected by the Project other than the Additional Information.

10.3 Maddocks has assumed that an amendment to the Regulation, with provisions as described in this PIA, will be made before any Additional Information is collected from schools.

11. Glossary

11.1 In addition to terms defined elsewhere in this PIA, the following acronyms and terms have the following meanings:

Acronyms	
APP	Australian Privacy Principle
ISM	Australian Signals Directorate Information Security Manual
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment
PSPF	Australian Government Protective Security Policy Framework

Definitions	
APP Guidelines	The APP Guidelines published by the OAIC at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/.
Personal Information	Means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not (see s 6, Privacy Act).
Privacy Act	The *Privacy Act 1988* (Cth).
PIA Guide	The OAIC's PIA Guide, available at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments. The procedure used in this PIA is consistent with the PIA Guide.

Attachment 1 APP Compliance

Below is an analysis of key elements of the APPs that are relevant to the Additional Information collected in the Project. The analysis does not address those elements of the APPs which reflect the Department's broader compliance obligations, but which do not specifically relate to the Additional Information.

1. APP 1 – open and transparent management of personal information

Text of APP 1

Australian Privacy Principle 1 — open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Analysis of compliance with APP 1

1.1 APP 1 is intended to ensure that entities manage Personal Information in an open and transparent way. Implementation of APP 1, including the adoption of an APP privacy policy, is a responsibility of the Department. Undertaking PIAs such as this one represents one reasonable step for the Department to take to implement practices, procedures and systems to comply with the APPs, as required under APP 1.2(a) and the *Privacy (Australian Government Agencies - Governance) APP Code 2017*. APP 1.4 requires the Department to adopt an APP privacy policy which contains a range of information.

1.2 This PIA does not consider the Department's privacy policy as it is outside of the scope of this PIA. However, nothing in the Project prevents compliance with APP 1.

2. APP 2 – anonymity and pseudonymity

Text of APP 2

Australian Privacy Principle 2 — anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Analysis of compliance with APP 2

2.1 The Department will only be required to deal with individuals in circumstances where the school contacts the Department to request correction of an individual's Additional Information. To allow the Department to correct the Additional Information, the school must identify the individual and a pseudonym would be impractical.

2.2 APP 2 is satisfied because, in accordance with APP 2.2(b), it is impractical for the Department to deal with individuals who have not identified themselves or who have used a pseudonym.

3. APP 3 – collection of solicited personal information

Text of APP 3

Australian Privacy Principle 3 — collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation — the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department — the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise — the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Analysis of compliance with APP 3

3.1 The Additional Information in the Project, for the purposes of APP 3.7, will be solicited by the Department through the relevant non-government schools. Pursuant to paragraph 3.6 of Chapter 3 of the APP Guidelines, *'an APP entity 'solicits' personal information 'if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included'.*

Collection permitted under APP 3.1

3.2 The Department may only collect Personal Information (other than sensitive information) that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1).

3.3 Determining whether a collection of Personal Information is permitted under APP 3.1 requires a two-step process:

Step 1 – identifying an entity's functions or activities; and

Step 2 – determining whether the relevant collection of Personal Information is reasonably necessary for or directly related to one of those functions or activities.[2]

3.4 Collection of information about schools and their students, which schools are required to provide under the Act and Regulation, is part of the Department's statutory functions and activities. As the Act and the Regulation (if amended) will authorise the Department to collect the Additional Information, the collection of Additional Information as part of the Project is reasonably necessary and directly related to that function.

3.5 We therefore consider that APP 3.1 is satisfied.

Application of APP 3.3 and APP 3.4

3.6 As the Additional Information is not sensitive information, APP 3.3 and APP 3.4 are not relevant.

Means of collection (APP 3.5)

3.7 Under APP 3.5, an entity must collect Personal Information 'only by lawful and fair means'.

3.8 A collection of Personal Information is lawful if it is not contrary to law. Conversely, a means of collection will not be lawful if a law, legal order or legal principle prevents that means of collection.

3.9 As the collection of the Additional Information will be authorised by the Regulation (if amended as proposed), and no law, legal order or legal principles prevent the Department from collecting the Additional Information in the manner proposed, the collection will therefore be by 'lawful means'.

3.10 A 'fair means' of collecting Personal Information is one that is not oppressive, does not involve intimidation or deception, and is not unreasonably intrusive. Whether a collection uses unfair means would depend on the circumstances. A collection of Personal Information may, for example, be unfair if it involves:

(a) collecting from a file accidentally left on a street or from a lost electronic device;

(b) collecting from an individual who is traumatised, in a state of shock or intoxicated;

(c) misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information; or

(d) collecting by telephoning an individual in the middle of the night.[3]

3.11 We do not consider that the collection of Additional Information by the Department constitutes collection by unfair means.

[2] APP Guidelines, Chapter 3, paragraphs 3.8 – 3.9.
[3] APP Guidelines, Chapter 3, paragraphs 3.62 – 3.63.

3.12 We therefore consider that APP 3.5 is satisfied.

Collecting directly from the individual (APP 3.6)

3.13 We note that the Project requires the Department to collect Additional Information from someone other than the individual (i.e., the school). This means that, under APP 3.6, the consent of the individual will be required, unless the Department is authorised by law to make that collection or it is unreasonable or impractical to collect the information directly from the individual.

3.14 As noted in paragraph 5.4 of this PIA, the Department will be authorised, under the Act and the amended Regulation, to collect the Additional Information from the school, meaning that APP 3.6 will be satisfied.

4. APP 4 – dealing with unsolicited personal information

Text of APP 4

Australian Privacy Principle 4 — dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

Analysis of compliance with APP 4

4.1 APP 4 only applies where the Department receives unsolicited Personal Information, i.e. information that it receives but has taken no active steps to solicit. This might include, for example, misdirected mail, unsolicited correspondence or job applications, or promotional fliers.

4.2 We consider that there is only a very low risk that any unsolicited Personal Information will be collected in relation to the Project. In the unlikely event that the Department does receive unsolicited Personal Information, it must manage it in a way that complies with APP 4. The Department may wish to provide staff with training surrounding how to deal with unsolicited Personal Information in the manner required by APP 4.

5. APP 5 – notification of the collection of personal information

Text of APP 5

Australian Privacy Principle 5 — notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h)	that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
(i)	whether the APP entity is likely to disclose the personal information to overseas recipients;
(j)	if the APP entity is likely to disclose the personal information to overseas recipients — the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Analysis of compliance with APP 5

5.1 APP 5 requires an entity that collects Personal Information about an individual to take reasonable steps to notify the individual of certain matters (referred to as 'APP 5 matters'), or otherwise ensure that the individual is aware of those matters. This notification must occur at or before the time of collection, or as soon as practicable afterwards.

5.2 The 'reasonable steps' test is an objective test, that considers whether a reasonable person in those circumstances would agree that the entity had acted reasonably in providing notice or ensuring awareness of the APP 5 matters. The reasonable steps for an entity will depend on circumstances that include:

(a) the type of Personal Information collected, including whether it comprises of any sensitive information;

(b) the possible adverse consequences for an individual as a result of the collection;

(c) any special needs of the individual; and

(d) the practicability, including time and cost involved (although the entity is not automatically excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so, and whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances).[4]

5.3 The OAIC has suggested that reasonable steps that an entity could consider include:

(a) if an entity collects Personal Information directly from an individual who completes a form or uses an online facility – clearly and prominently displaying the APP 5 matters in the form or providing a readily accessible link to an APP 5 notice, and asking the individual to confirm that they have reviewed the notice before collecting their Personal Information;

(b) if Personal Information is collected by telephone, explaining the APP 5 matters to an individual at the start of the call;

(c) if the entity collects Personal Information from another entity, ensuring that the other entity has notified or made the individual aware of the relevant APP 5 matters (such as through an enforceable contractual arrangement); or

[4] APP Guidelines, Chapter 5, paragraph 5.4.

(d) where it is not reasonable to notify or ensure awareness of the full range of APP 5 matters, alerting the individual to specific sections of its APP privacy policy or other general documents containing relevant information.[5]

5.4 However, the OAIC notes that *'it may be reasonable for an APP entity not to take any steps to provide a notice or ensure awareness of some or all of the APP 5 matters'*[6]. The OAIC further notes that an example of when it may be reasonable for an APP not to take any steps or provide a notice or ensure awareness of some or all of the APP 5 matters may be that the *'the individual is aware that personal information is being collected, the purpose of collection and other APP 5 matters relating to the collection'*[7].

5.5 Under the Project the Department is not collecting the Additional Information from the individuals concerned. The relevant schools collate this information, which is typically already held by the school, and upload the information into the SEP portal.

5.6 The Department provides each relevant non-government school with a Project Collection Notice that is to be provided, in a manner the school considers appropriate, to each parent/guardian affected by the collection of the Additional Information.

5.7 The Department requires relevant non-government schools to declare that *'A Statement of Address Notice has been provided to the parent or legal guardian of each student for whom a residential address has been submitted'* prior to submitting the data through the SEP Portal.

5.8 Requiring schools to provide the Project Collection Notice, and seeking confirmation from the schools that this has been done, are reasonable steps for the Department to take in order to ensure that individuals are aware of the relevant APP5 matters. It is also reasonable for the Department to permit schools to decide how best to distribute the Project Collection Notice to individuals, given a school will be best placed to determine this in light of their particular communication channels.

5.9 We have also reviewed the Project Collection Notice and we note that it does not contain all of the APP 5 matters. The Project Collection Notice does not:

(a) provide that the Department's privacy policy contains information about how an individual may access their Personal Information, and seek correction of such information (APP 5.2(g));

(b) provide that the Department's privacy policy contains information about how an individual may complain about a privacy breach, and how the Department will deal with such a complaint (APP 5.2(h)); and

(c) provide whether the Department is likely to disclose the Personal Information to overseas recipients (APP 5.2(i)).

5.10 We **recommend** that the Department consider amending the Project Collection Notice to ensure that it contains all of the APP 5 matters. To assist, we have included an amended Project Collection Notice at Attachment 2**.**

[5] APP Guidelines, Chapter 5, paragraph 5.6.
[6] APP Guidelines, Chapter 5, paragraph 5.7.
[7] APP Guidelines, Chapter 5, paragraph 5.7.

6. APP 6 – use or disclosure of personal information

Text of APP 6

Australian Privacy Principle 6 — use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information — directly related to the primary purpose; or

(ii) if the information is not sensitive information — related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

Analysis of compliance with APP 6

6.1 APP 6 provides that an entity must not use or disclose Personal Information that was collected for a primary purpose, for another purpose (secondary purpose), unless the individual has consented to the use or disclosure of the information, or APP 6.2 or APP 6.3 applies.

6.2 Additional Information collected by the Department in relation to the Project will be used and disclosed by the Department in relation to its primary purposes, that is, to assist in the development of a new SES score methodology and to inform future policy development, in accordance with the Act and the Regulation (as it is proposed to be amended).

6.3 The primary purpose is explicitly communicated to individuals through the Project Collection Notice.

Disclosure for a secondary purpose

6.4 The Department will also potentially disclose the Additional Information collected as part of the Project for a number of secondary purposes:

(a) arguably, the disclosure to the ABS for the MADIP project may be seen as a secondary purpose (although we note that there is an alternative argument that this is simply a mechanism to facilitate use by the Department for the primary purpose, but we have considered it as a secondary purpose for the purposes of this PIA to ensure full consideration);

(b) to external contractors who need to audit or verify student records to ensure that information that a school provides to the Department is accurate; and

(c) to its ICT services provided (engaged by the Department of Jobs and Small Business), if access is required for the purposes of administering the infrastructure on which the Additional Information is stored and providing ICT support services.

6.5 Importantly, APP 6.2(b) provides that the restriction in APP 6.1 does not apply if *'the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order'*.

6.6 The Act and the Regulation (if amended as proposed) will authorise the Department to collect Additional Information in the Project. Section 6 of the Act defines *'information obtained under or for the purposes of this Act'* as *'school education information'*. The Additional Information meets this definition of 'school education information'.

6.7 As set out in paragraphs 6.1 and 6.2 of the PIA, section 125 of the Act and section 65 of the Regulation authorise the use and disclosure of school education information:

(a) for the purposes of the Act or the Regulation;

(b) for programs administered by the Minister;

(c) for research into matters of relevance to the Department;

(d) statistical analysis of mattes of relevance to the Department; and

(e) policy development,

as well as expressly permits disclosure of school education information to the ABS for the purposes of the ABS's functions.

6.8 Accordingly, it is likely that disclosure to the ABS for the purposes of the particular MADIP project, and to contracted auditors to ensure compliance with the requirements of the Act or the Regulation, is (or will be if the proposed amendment to the Regulation is made) authorised by law so that the prohibition in APP 6.1 will not apply.

6.9 In addition, APP 6.3 provides that the prohibition in APP 6.1 will not apply if the individual would reasonably expect the Department to use the Additional Information for a secondary purpose related to the primary purpose[8]. Whether an individual reasonably expects their Personal Information to be used or disclosed for a secondary purpose is an objective test based on the individual circumstances. It is certainly arguable that, in the circumstances of the Project, the individuals about whom the Department collects the Additional Information would reasonably expect it to be stored on the Department's ICT systems, and that it is commonly known that maintenance and support of Commonwealth ICT infrastructure by service providers is standard business practice.

6.10 This means that Department could conclude that individuals would reasonably expect the Additional Information to be used and disclosed to a support services provider for the purposes of maintaining the Department's ICT system on which the Additional Information is stored. We consider the purpose of maintaining the ICT system that enables the primary purpose of collection (i.e., the use of the Additional Information for further policy development) to be directly related to that primary purpose.

6.11 However, for completeness, we **recommend** that the Project Collection Notice be amended to explicitly state that the Department may disclose Personal Information to its service providers (including to the Department of Jobs and Small Business for the purpose of providing ICT support services in relation to the Project, or relevant external auditors for compliance purposes).

6.12 The Department should also ensure that its contractual and other arrangements with those service providers contain appropriate requirements for the protection of Personal Information (including the Additional Information).

Function creep

6.13 We note that there is always a risk of 'function creep', where information which is directly related to the primary purpose starts to be used for another purpose which was not originally anticipated. This is particularly relevant in terms of future use of the Additional Information, and the de-identified data sets received from the ABS as a result of the MADIP project.

6.14 We **recommend** that the Department consider implementing processes and governance arrangements to ensure that function creep does not occur. For example, the Department could undertake a periodic review to confirm that Additional Information collected in the Project continues to be used by the Department solely for the purpose of:

(a) undertaking analysis to support the development of a potential new SES score methodology, as recommended by the National School Resourcing Board; and

(b) assisting with other policy development

6.15 If future uses of the Additional Information are proposed, we recommend that this PIA be reconsidered and updated as needed.

[8] As the Additional Information is not sensitive information, the secondary purpose does not need to be 'directly related' to the primary purpose.

7. APP 7 – direct marketing

Text of APP 7

Australian Privacy Principle 7 — direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions — personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception — sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception — contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies — request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies — request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d) — the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e) — the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

Analysis of compliance with APP 7

7.1 APP 7 applies to 'organisations' as defined in the Privacy Act, rather than to agencies like the Department.

7.2 Under section 7A of the Privacy Act, an act or practice of an agency may in the prescribed circumstances be treated as an act or practice of an organisation. This applies to:

(a) a prescribed agency specified in Part I of Schedule 2 to the *Freedom of Information Act 1982* (**FOI Act**); or

(b) an agency specified in Division 1 of Part II of Schedule 2 to the FOI Act.

7.3 The Department is not one of the agencies specified under section 7A of the Privacy Act.

7.4 As APP 7 does not apply to the Department, it is not necessary to address use of Additional Information collected by the Department for the purposes of the Project for direct marketing purposes in this PIA.

8. APP 8 – cross-border disclosure of personal information

Text of APP 8

Australian Privacy Principle 8 — cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.

Analysis of compliance with APP 8

8.1 The Department does not intend to disclose any Personal Information collected as part of the Project to any overseas recipient.

8.2 The Additional Information will be stored electronically on infrastructure provided and managed by the Department of Jobs and Small Business, under an MOU, as part of a shared services agreement.

8.3 The Department has advised that:

(a) the relevant Department of Jobs and Small Business' ICT infrastructure, including that used for hosting the SEP portal, is located within Australia; and

(b) as all Department of Jobs and Small Business support personnel with access to the Project have security clearances, we understand that:

(i) they have Australian citizenship; and

(ii) by virtue of their security clearance, cannot perform their roles in relation to the Project outside Australia.

8.4 It is therefore reasonable to assume that the ICT infrastructure on which the Additional Information is stored, and all associated support personnel with access to the Project, are located within Australia.

9. APP 9 – adoption, use or disclosure of government related identifiers

Text of APP 9

Australian Privacy Principle 9 — adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Analysis of compliance with APP 9

9.1 APP 9 applies to 'organisations' rather than agencies, except in the limited circumstances set out in section 7A of the Privacy Act (which are not relevant to the Department). It is therefore not necessary to consider APP 9 in the context of the Project.

10. APP 10 – quality of personal information

Text of APP 10

Australian Privacy Principle 10 — quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Analysis of compliance with APP 10

10.1 Under APP 10, the Department needs to determine what steps (if any) are reasonable for it to take to verify that the Personal Information collected in the Project is accurate, up to date, complete and relevant.

10.2 In the context of APP 10, the 'reasonable steps' that an entity should take will depend upon circumstances that include:

(a) the sensitivity of the Personal Information;

(b) the nature of the entity (including its size, resources and business models);

(c) the possible adverse consequences for an individual if the quality of Personal Information is not ensured; and

(d) the practicability, including time and cost involved. However, an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.[9]

10.3 It is implicit in the use of the phrase 'if any' in APP 10.1 that it will be reasonable for an entity to take no steps to ensure data quality in some circumstances. For example, where an entity collects Personal Information from a source known to be reliable (such as the individual concerned) it may be reasonable to take no steps to ensure data quality.[10]

10.4 To verify the quality of the information collected as part of the Project, including the Additional Information, the Department undertakes a quality assurance process. The Department uses information previously collected by the Department about the school to check that there are no obvious anomalies in the data. The previously collected information comprises aggregated data only, and does not contain any Personal Information.

10.5 Given the nature of the Additional Information collected, and the fact that schools provide the Additional Information in accordance with the applicable legislation to determine funding, and on the understanding that the school may be subject to an audit, we consider the Department's approach to ensuring the quality of the Additional Information collected for the purposes of the Project, is reasonable in the circumstances.

11. APP 11 – security of personal information

Text of APP 11

Australian Privacy Principle 11 — security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

[9] APP Guidelines, Chapter 10, paragraph 10.6.
[10] APP Guidelines, Chapter 10, paragraph 10.7.

Analysis of compliance with APP 11

11.1 APP 11.1 requires an APP entity to take such steps as are reasonable to protect Personal Information from misuse, interference and loss, and from unauthorised access, modification or disclosure. The term 'reasonable' is not defined in the Privacy Act, but the APP Guidelines provide that the term bears its ordinary meaning, as being based upon or according to reason and capable of sound explanation.[11] What is reasonable can be influenced by current standards and practices.[12]

11.2 The Department applies security policies and procedures in respect of the Project. These include:

(a) access to the Project being restricted only to Departmental personnel who have been duly authorised; and

(b) data security in relation to storage of the Additional Information , governed by the Department of Jobs and Small Business; and

(c) additional security protections in relation to the secure transmission of the Additional Information to the ABS.

11.3 These security measures have been assessed by the Department as sufficiently secure in light of the nature of the Personal Information held. The application of these measures will generally constitute such steps as are reasonable in the circumstances to protect the Additional Information from misuse, interference and loss and unauthorised access, modification or disclosure, sufficient to demonstrate compliance with APP 11.

11.4 As we understand that the Additional Information held in the Project is contained in a Commonwealth record, the requirements of APP 11.2 do not apply.

12. APP 12 – access to personal information

Text of APP 12

Australian Privacy Principle 12 — access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access — agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

[11] APP Guidelines, Chapter B, paragraph B.105.
[12] *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20 (Mason, Wilson and Dawson JJ at paragraph 12).

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access — organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency — within 30 days after the request is made; or

(ii) if the entity is an organisation — within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Analysis of compliance with APP 12

12.1 Under APP 12, an APP entity is required to give an individual access to the Personal Information held by it unless it is authorised by legislation to refuse access. The exceptions to access in APP 12.3 only apply to 'organisations', and do not apply to the Department as the Department is not an organisation as defined under section 7A of the Privacy Act.

12.2 The Department must give the individual access to their Personal Information within 30 days of request, and in the form reasonably requested by the individual. The Department cannot charge the individual for making the request or access being given by the Department.

12.3 If the Department refuses to give access to the Personal Information at all (because the Department is authorised to refuse access under the FOI Act or other Commonwealth legislation) or to give access to the information in the manner requested by the individual, the Department must take reasonable steps to give access in a way that meets the needs of the Department and the individual. This might involve access through the use of an intermediary or access to a redacted document.

12.4 We understand that nothing in the Project prevents the Department from complying with APP 12.

13. APP 13 – correction of personal information

Text of APP 13

Australian Privacy Principle 13 — correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(b) if the entity is an agency — within 30 days after the request is made; or

(c) if the entity is an organisation — within a reasonable period after the request is made; and

(d) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

Analysis of compliance with APP 13

13.1 The Department can update or correct Additional Information in the Project simply by correcting the Additional Information in the SEP portal, if requested to do so by a school.

13.2 We understand that nothing in the Project would prevent the Department from complying with APP 13.

Attachment 2 Project Collection Notice

Australian Government
Department of Education and Training

2018 Residential Address Collection Notice

This notice is from the Australian Government Department of Education and Training (the **department**), to advise you that the department has requested that your child's school provide a *statement of addresses*, in accordance with the *Australian Education Regulation 2013* (Cth) (the **Regulation**).

A *statement of addresses* contains the following information about each student at the school:

- Student residential address **(not student names)**
- Student level of education (i.e. whether the student is a primary or secondary student)
- Student boarding school status (i.e. whether the student is boarding or a day student)
- Names and residential addresses of the student's parent(s) and/or guardian(s)

Schools generate a record number for each student for the purposes of this collection, which is also provided to the department.

Purpose of the collection

This collection is routinely used to inform Commonwealth school education policy, and to help ensure that Commonwealth funding arrangements for non-government schools are based on need, and are fair and transparent.

The National School Resourcing Board recently completed a review of the socio-economic status (**SES**) score methodology used in the calculation of the Commonwealth's needs-based funding arrangements for non-government schools. The information collected in the *statement of addresses* will be used to consider the Board's recommendations. Further information on this review can also be found here: https://www.education.gov.au/review-socio-economic-status-ses-score-methodology.

Use and disclosure of personal information

Your personal information is protected by law, including the *Privacy Act 1988* (Cth). Any use and disclosure of your personal information relating to the *statement of addresses* will occur in accordance with the Regulation.

Your personal information may be used by the department, or disclosed to the Australian Bureau of Statistics (the **ABS**), for the purposes of SES score policy development, reviewing SES score methodology, calculating SES scores, Commonwealth school education policy development (including school funding), or where it is otherwise required or authorised by law.

For example, your personal information may be provided to the ABS for statistical and research purposes, which includes data integration projects such as the Multi-Agency Data Integration Project (MADIP). Further information on the MADIP can be found here: http://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP.

The department may, from time to time, carry out audits of school submissions. In the event of an audit, contracted auditors may seek to compare a school's *statement of addresses* with student enrolment information held by the school. These contractors will not use the information for any other purpose.

The department may also be required to disclose your personal information to contracted providers for the purposes of the provision of ICT support services to the department.

The department does not intend to disclose personal information to overseas recipients.

What do you need to do?

You are not required to do anything. Your school is responsible for providing the requested details to the department, however, please ensure that your school has the most up-to-date and correct details for your family.

Contacts for further information

Your school can provide additional information about the process for the *statement of addresses* collection.

If you have any further questions regarding the collection, you can contact the department by:

- Email: seshelpdesk@education.gov.au
- Phone (free call): SES helpdesk on 1800 677 027 (Option 4)

The department's privacy policy is available on the department's website at www.education.gov.au. The privacy policy contains information about:

- how individuals can access and seek correction of the personal information held by the department;
- how complaints about breaches of the *Privacy Act 1988* (Cth) can be made; and
- how the department will deal with these complaints.

If you wish to contact the department about privacy-related matters, please email the department at EducationPrivacy@education.gov.au or write to:

Privacy Contact Officer
Schools, Childcare and Corporate Legal Branch
Department of Education and Training
GPO Box 9880
Canberra ACT 2601