ABS abides by the Privacy Act 1988 (Commonwealth) and (from 12 March 2014), the Australian Privacy Principles (APPs) and keeps student information private, only collecting information that relates to a student’s training and will take all reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure including restricted access to electronic files, secure storage of paper files and back up of data.

Information collected by the Australian Business School is protected by the Privacy Amendment (Private Sector) Act 2000 (Cth). Information collected by this form is for the purpose of obtaining details to assist us in providing goods and services and will not be disclosed to a third party, except where prior written permission is obtained from the individual who supplied the information and to whom the information refers.

1. **COLLECTION**

ABS will only collect personal information that is necessary for one or more of its functions or activities. ABS will only collect personal information by lawful and fair means and not in an unreasonably intrusive way.

If it is reasonable and practicable to do so, ABS will collect personal information about an individual only from that individual.

2. **USE & DISCLOSURE**

ABS will not use or disclose personal information about an individual for a purpose other than the primary purpose of collection unless:
(a) Both of the following apply:

(i) The secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) The individual would reasonably expect ABS to use or disclose the information; or

(b) The individual has consented to the use or disclosure; or

(c) If the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

   I. It is impracticable for ABS to seek the individual's consent before that particular use;
   II. ABS will not charge the individual for giving effect to a request by the individual to ABS not to receive direct marketing communications;
   III. The individual has not made a request to ABS not to receive direct marketing communications;
   IV. In each direct marketing communication with the individual, ABS draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(d) ABS reasonably believes that the use or disclosure is necessary to lessen or prevent:

   I. A serious and imminent threat to an individual's life, health or safety; or
   II. A serious threat to public health or public safety; or

(e) ABS has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(f) The use or disclosure is required or authorised by or under law; or

3. DATA QUALITY

ABS will take reasonable steps to make sure that the personal information it collects uses or discloses is accurate, complete and up-to-date.

4. DATA SECURITY

ABS will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. ABS will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed.
5. **ACCESS AND CORRECTION**

If ABS holds personal information about an individual, it will provide the individual with access to the information on request by the individual, in a form or manner suitable to the individual’s reasonable needs, except to the extent that:

(i) Providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) Providing access would be likely to prejudice:

(i) The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) The enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) The protection of the public revenue; or

(iv) The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) The preparation for, or conduct of, proceedings before any court or tribunal, or implementation or its orders;

By or on behalf of an enforcement body; or

(k) An enforcement body performing a lawful security function asks ABS not to provide access would be likely to cause damage to the security of Australia.

However, where providing access would reveal evaluative information generated within ABS in connection with a commercially sensitive decision-making process, ABS may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

If ABS levies charges for providing access to personal information, those charges:

(a) Will not be excessive; and

(b) Will not apply to lodging a request for access.

7. **IDENTIFIERS**

ABS will not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) An agency; or

(b) An agent of an agency acting in its capacity as agent; or

(c) A contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

ABS will not use or disclose an identifier assigned to an individual by an agency or by an agent or contracted service provider mentioned above) unless:
(a) The use of disclosure is necessary for ABS to fulfil its obligations to the agency; or
(b) The use of disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

8. ANONYMITY

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9. TRANSBORDER DATA FLOWS

ABS will transfer personal information about an individual to someone (other than ABS or the individual) who is in a foreign country only if:

(a) ABS reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to ABS’s Privacy Protection Principles;
(b) The individual consents to the transfer;
(c) The transfer is necessary for the performance of a contract between the individual and ABS, or for the implementation of pre-contractual measures taken in response to the individual’s request;
(d) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between ABS and a third party;
(e) All of the following apply:
   (i) The transfer is for the benefit of the individual; and
   (ii) It is not practicable to obtain the consent of the individual to that transfer; and
   (iii) If it were practicable to obtain such consent, the individual would be likely to give it;
   (f) ABS has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with ABS’s Privacy Protection Principles.

10. SENSITIVE INFORMATION

ABS will not collect Sensitive Information about an individual unless:

(a) The individual has consented; or
(b) The collection is required by law; or
(c) The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

   (i) is physically or legally incapable of giving consent to the collection; or
   (ii) Physically cannot communicate consent to the collection; or

(d) If the information is collected in the course of the activities of a non-profit organisation – the
following conditions are satisfied:

(i) The information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) At or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individuals consent; or

(e) The collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

ABS will take reasonable steps to permanently de-identify the information before ABS discloses it.

Freedom of Information:

From 1 July 2009, the Right to Information Act 2009 replaced the Freedom of Information Act 1992 and is part of a broader “push” model of greater proactive and routine release of information. The RTI Act provides a right of access to government information unless, on balance, it is contrary to the public interest to release the information. More information on the RTI Act can be accessed here: www.rti.qld.gov.au.

2. Purpose

The purpose of this policy is to explain how the Australian Business School ABS collects and keeps student information private and abides by the Privacy Act 1988 (Commonwealth) and (from 12 March 2014), the Australian Privacy Principles (APPs).

3. Scope

The scope of this policy and procedure applies to all students, stakeholders and employees of ABS. This procedure applies to all the following materials either printed, electronically communicated, electronic media where a client gives or supplies personal information.

4. Definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABS</td>
<td>Australian Business School</td>
</tr>
<tr>
<td>DoS</td>
<td>Director of Studies</td>
</tr>
<tr>
<td>DIBP</td>
<td>Department of Immigration and Border Protection</td>
</tr>
<tr>
<td>RPL</td>
<td>Recognition of Prior Learning</td>
</tr>
<tr>
<td>APP</td>
<td>Australian Privacy Principles</td>
</tr>
</tbody>
</table>
Personal Information - Information held by ABS could include:

- Student name
- Students USI (Unique Student Identifier)
- Current & previous address
- Telephone numbers
- Email address
- Drivers license number
- Bank account details
- Passport number
- Assessment results
- Counselling or intervention strategies
- File notes

5. Procedures

1. Familiarise self with internal privacy policies and procedures.
   
   a) Understand your personal information handling processes and procedures and undertake regular privacy training. Following internal processes and procedures will help you manage and mitigate privacy risks, including the risks posed by human error.
   
   b) Read your privacy policy and ensure you understand how it applies to the way you handle personal information.
   
   c) Make sure you provide privacy notices to customers and that you handle their personal information in the way you say you will.

2. Know who is responsible for privacy

   a) Everyone has a role to play in ensuring privacy is respected and protected. There should be a senior member of staff with overall accountability for privacy. There should also be staff responsible for managing privacy, including a key privacy officer, who:

      I. understands your entity’s responsibilities under the Privacy Act
      II. handles access and correction requests and complaints and enquiries about your personal information handling practices.

   b) If your workplace is small, the key privacy officer may hold this role as part of their broader responsibilities.
   
   c) If you notice any issues with privacy processes and procedures, discuss it with the key privacy officer or someone senior.
3. Consider privacy during project planning

When developing a project that involves new or changed personal information handling practices, always consider doing a privacy impact assessment (PIA). A PIA identifies how a project can have an impact on individuals’ privacy, and makes recommendations for managing, minimising or eliminating privacy impacts. You should also engage your key privacy officer during the planning phase of your project.

4. Only collect the personal information you need

You must only collect personal information that you actually need. Don’t collect personal information just because it may become necessary or useful at a later date. If you need it later, you can collect it then.

5. Use and disclosure — think about it!

a) Generally, you are only allowed to use or disclose personal information for the primary purpose for which it was collected. However, there are exceptions that allow for it to be used or disclosed for another purpose. These exceptions include where:

   I. the individual has consented to the use or disclosure
   II. the individual would reasonably expect the use or disclosure and the other purpose relates (or for sensitive information, directly relates) to the primary purpose of collection
   III. the use or disclosure is required or authorised by law.

b) Always think about whether you can conduct your business activities without using or disclosing personal information. When you do, always limit the amount of personal information you use or disclose to the minimum necessary.

6. Overseas disclosure — prepare for it!

Before you disclose personal information to an overseas recipient, you must take reasonable steps to ensure that the recipient complies with the APPs (although there are some exceptions, which are outlined in APP guidelines Chapter 8). These may include entering into an enforceable contractual arrangement that requires the overseas recipient to handle the personal information in accordance with the APPs (except for APP 1).

7. Take care when handling sensitive information

a) Sensitive information is given a higher level of privacy protection under the Privacy Act and you have additional responsibilities when you collect, use or disclose it.

b) Sensitive information is a specific set of personal information that includes an individual’s racial or ethnic origin, religious beliefs or affiliations and sexual orientation or practices. Generally, sensitive information can only be collected with someone’s consent.
8. Access personal information on a need-to-know basis

Generally, you should only have access to personal information that you need for your role or function. By limiting the personal information you and your staff access to that needed, you are helping to protect the information from unauthorised access, use or disclosure.

9. Keep personal information secure

You must take reasonable steps to protect personal information from unauthorised access, modification or disclosure and also against misuse, interference and loss. You must also take reasonable steps to destroy or de-identify personal information when it is no longer needed for any purpose permitted under the Privacy Act.

10. Respond to the request for access to the personal information

Respond to the request for access to the personal information within a reasonable period after the request is made; and give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

11. Deal with complaint about a breach of the Australian Privacy Principles

1. The student is to fill in the form Privacy Complaints Form.
2. The form is either submit the form to the
   a. Reception of the Australian Business School, or,
   b. the Director of Studies Australian Business School
3. The complaint will be recorded in the Information Request Spreadsheets under the tab “Complaints Privacy Register”.
4. If the matter is not resolved then the issue can be referred to the Privacy Commissioner: 1300 363 992;

6. Responsibilities

6.1 DoS VET, CEO, Marketing, Trainers, Administration
5. Ensure ABS deals with information in compliance with the legislation, principles, policy and procedure above.

7. Documentation

7.1 Privacy Complaints Form