

PRIVACY POLICY

Butler McIntyre Investments Ltd
ACN 091 407 046
responsible entity for the Butler McIntyre Mortgage Fund

1 INTRODUCTION

1.1 Key Definitions

Term	Explanation
BMI	means Butler McIntyre Investments Ltd ACN 091 407 046 ('Company') (together, 'BMI' or 'we' or 'us')
Fund	means Butler McIntyre Mortgage Fund ARSN 094 635 720.
APP	means the Australian Privacy Principles set out in the <i>Privacy Act 1988</i> (Cth).
Board	means the Board of Directors of BMI.

1.2 Background

BMI collects and holds personal information about shareholders, borrowers and investors, in regard to their identification, assets and liabilities, income and expenditure, personal circumstances, and other similar information as required or appropriate for BMI to consider investment and loan applications.

1.3 Collection of information

We collect the information from individuals, companies and other entities, by their submissions and requests to interact with the Company or Fund, when they seek to invest, contract with, borrow from, or deal with us. We collect it either by paper documentations, letters, correspondence, files of financial data, or the same type of material delivered electronically. We also collect information about individual borrower applicants by our due diligence process of applying for financial integrity data from external information providers and collectors, and from public registries.

1.4 Storage of Information

- (a) We hold the information in paper files or electronic files, indexed in accordance with usual office procedures, in filing cabinets or on computer hard-drives, and store the information in our offices and storage repositories in Hobart.
- (b) We collect the information about individuals in order that we can attend to our business of running and managing a public company, in obeying the laws of Australia to have and keep up to date registries of information about the company, and to obey financial and accounting obligations of the business. In regard to the Fund, we collect the information in order to make decisions about whether to accept investments or to agree to lending money of the Fund, in our obligations in making decisions in accordance with our constituent documents: the mortgage Fund constitution, our Compliance Plan, and policies and practices established to ensure investments are properly managed and accounted for, and borrowings are

authorised and managed in a safe manner.

1.5 Disclosure of information

We disclose such information within the Company and the Fund management (including our Compliance Committee) as part of our business processes. We disclose some of the information to auditors and regulatory agencies as required by law (notably the Corporations Act). Normally the information is kept confidential within the Company and the Fund, but is amenable to being required to be disclosed pursuant to legislative or court process.

1.6 Obtaining information

If an individual wishes to procure information which we hold about them they may apply ('contact us') to either the Investment and Lending Manager, or the Director (Statutory Compliance). They may do so by telephoning our office on 03 6222 9444, by email to enquiry@bmil.com.au, or by letter addressed to GPO Box 980, Hobart, Tasmania, 7001.

1.7 Review and revision of information

- (a) If an individual believes information we hold in relation to them is incorrect, they may apply to correct that information by providing us with written advice as to their perception as to the error in the information. We will consider the advice, and if appropriate, will correct the information, and will reconsider any decision or judgment we have made in relation to the individual on the basis of the corrected information. The written advice should be directed as above, either by email or letter; and
- (b) If an individual perceives we are in breach of the Australian Privacy Principles, they may contact us and inform us how they perceive we are in breach. We will review the assertion, will inform the individual of whether we agree or disagree with their assertion that we are in breach, and we will take remedial action (if appropriate) in regard to our policies, processes and administration to avoid the breach continuing or being repeated. We will inform the individual of the nature of the remedial action we take.

1.8 Overseas recipients

We do not disclose personal information to overseas recipients (except about an individual to that individual).

1.9 Privacy law of Australia requires:

APP Privacy policy extract:

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.*

APP Source:

February 2013 (amended January 2014)

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

This is the text of the 13 APPs from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988. For the latest versions of these Acts visit the ComLaw website: www.comlaw.gov.au.

APP set out below:

Dated March 2016

Approved by the Board of BMI

They are binding on us, and we will take reasonable steps to implement practices, procedures and systems to meet those obligations.

Australian Privacy Principles

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

1.1 Open and transparent management of personal information

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

1.2 Compliance with the Australian Privacy Principles

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.

1.3 APP Privacy policy

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 Information combined

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.

1.5 Availability of the APP privacy policy

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 Request the APP privacy policy

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.

2 Australian Privacy Principle 2 — anonymity and pseudonymity

2.1 Option of identification

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 Exclusion of the option

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.

3 Australian Privacy Principle 3 — collection of solicited personal information

3.1 Personal information other than sensitive information

- (a) 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; and
- (b) 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.

3.2 Sensitive information

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

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.
- (c) Subclause 4.3 applies in relation to the information.

3.3 Requirements of sensitive information

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

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

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

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

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

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

- (i) the information relates to the activities of the organisation; and
- (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.

3.4 Means of collection

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

3.5 Means of collection about an individual

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

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

it is unreasonable or impracticable to do so.

3.6 Solicited personal information

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

4 Australian Privacy Principle 4 — dealing with unsolicited personal information

4.1 Unsolicited personal information

an APP entity receives personal information; and

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 Use or disclose unsolicited personal information

The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 5.1.

4.3 Collection of unsolicited personal information

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

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 Determination of unsolicited personal information

If subclause 5.3 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.

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

5.1 Notification of the collection of personal information

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:

to notify the individual of such matters referred to in subclause 6.2 as are reasonable in the circumstances; or

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

5.2 Matters for notification of the collection of personal information

The matters for the purposes of subclause 6.1 are as follows:

the identity and contact details of the APP entity;

Determined 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;

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);

the purposes for which the APP entity collects the personal information;

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

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;

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;

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;
- (ii) 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.

6 Australian Privacy Principle 6 — use or disclosure of personal information

6.1 Use or disclosure

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:

the individual has consented to the use or disclosure of the information; or

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 Use or disclosure of personal information about an individual

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

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

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

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

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

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 Use or disclosure of personal information by an agency

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

the agency is not an enforcement body; and

the information is biometric information or biometric templates; and

the recipient of the information is an enforcement body; and

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

6.4 Use or disclosure of personal information by an entity

The use or disclosure of personal information by an entity is relevant if:

the APP entity is an organisation; and

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 7.1 or 7.2.

6.5 Written note of use or disclosure

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.

6.6 Related bodies corporate

This subsection applies if:

an APP entity is a body corporate; and

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.

6.7 Exceptions

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

personal information for the purpose of direct marketing; or

government related identifiers.

7 Australian Privacy Principle 7 — direct marketing

7.1 Direct marketing

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.

7.2 Exceptions — personal information other than sensitive information

Despite subclause 8.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

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

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

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

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

the individual has not made such a request to the organisation.

7.3 Exception — sensitive information

Despite subclause 8.1, 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.

7.4 Exception — contracted service providers

Despite subclause 8.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

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

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

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

7.5 Individual may request not to receive direct marketing communications

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

for the purpose of direct marketing by the first organisation; or

for the purpose of facilitating direct marketing by other organisations;

the individual may:

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

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

request the first organisation to provide its source of the information.

7.6 Individual must not be charged

If an individual makes a request under subclause 8.5, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

if the request is of a kind referred to in paragraph 8.5(c) or (d) — the first organisation must give effect to the request within a reasonable period after the request is made; and

if the request is of a kind referred to in paragraph 8.5(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.

7.7 Interaction with other legislation

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

the Do Not Call Register Act 2006;

the Spam Act 2003;

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

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

8.1 Cross-border disclosure of personal information

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

who is not in Australia or an external Territory; and

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 Exemptions – cross-border disclosure of personal information

Subclause 9.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

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

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 9.1 will not apply to the disclosure;
- (ii) after being so informed, the individual consents to the disclosure; or

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

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

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

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.

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

9.1 Adoption of government related identifiers

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

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

subclause 10.3 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.

9.2 Use or disclosure of government related identifiers

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

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

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

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

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

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

subclause 10.3 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.

9.3 Regulations about adoption, use or disclosure

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

the identifier is prescribed by the regulations; and

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

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).

10 Integrity of personal information

10.1 Australian Privacy Principle 10 — quality of personal information

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 Regulations concerning the quality of personal information

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.

11 Australian Privacy Principle 11 — security of personal information

11.1 Security of personal information

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

from misuse, interference and loss; and

from unauthorised access, modification or disclosure.

11.2 Regulations concerning the security of personal information

The security of personal information is relevant if:

an APP entity holds personal information about an individual; and

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

the information is not contained in a Commonwealth record; and

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.

12 Australian Privacy Principle 12 — access to personal information

12.1 Access

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.

12.2 Exception to access — agency

the APP entity is an agency; and

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;
then, despite subclause 13.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

12.3 Exception to access — organisation

If the APP entity is an organisation then, despite subclause 13.1, the entity is not required to give the individual access to the personal information to the extent that:

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

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

the request for access is frivolous or vexatious; or

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

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

giving access would be unlawful; or

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

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

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

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

12.4 Dealing with requests for access

In order to deal with requests for access, the APP entity must:

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

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

12.5 Other means of access

If the APP entity refuses, the other means of access are:

to give access to the personal information because of subclause 13.2 or 13.3; or

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 Other modes of access

Without limiting subclause 13.5, access may be given through the use of a mutually agreed intermediary.

12.7 Access charges

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 Regulations concerning access charges

Access charges are applied if:

the APP entity is an organisation; and

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.

12.9 Refusal to give access

If the APP entity refuses to give access to the personal information because of subclause 13.2 or 13.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

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

the mechanisms available to complain about the refusal; and

any other matter prescribed by the regulations.

12.10 Requirement for the refusal to give access

If the APP entity refuses to give access to the personal information because of paragraph 13.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

13 Australian Privacy Principle 13 — correction of personal information

13.1 Correction

Correction of personal information is required if:

an APP entity holds personal information about an individual; and

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.

13.2 Notification of correction to third parties

Notification of correction to third parties is required if:

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

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.

13.3 Refusal to correct information

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:

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

the mechanisms available to complain about the refusal; and

any other matter prescribed by the regulations.

13.4 Request to associate a statement

Request to associate a statement is required if:

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

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.

13.5 Dealing with requests

If a request is made under subclause 14.1 or 14.4, the APP entity:

must respond to the request:

- (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

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).