CGL PRIVACY POLICY

Corporate Governance Policy

MAY 2015

The Citadel Group Limited
ACN 127 151 026

Content

1 CGL PRIVACY POLICY

1.1 INTRODUCTION

Owner:	The Chief Financial Officer
Approving Authority:	Managing Director, The Citadel Group
Approval Date:	25 March 2014
Accountability:	Subsidiary CEO/General Managers, Workforce Manager, Finance Team, Payroll Administrators and those responsible for contracts with Australian Government Agencies, clients, customers and students.
Users:	All employees across the Citadel Group including all subsidiary companies and business partners (CGL) responsible ensuring privacy principles are applied when dealing with the personal information of clients, customers, employees, independent contractors and students.
Purpose:	**Legal compliance with the Privacy Act 1988 and amendments in effect from 12 March 2014:** Establish the policy and procedural environment that treats all personal information in accordance with the Australian Privacy Principles (APP) for private sector organisations with an annual turnover of $3 million or more. For more information refer to the guideline at: http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP_guidelines_complete_version_1_March_2014.pdf

Acronyms

APP	Australian Privacy Principles
ASQA	Australian Skills Quality Authority
CGL	The Citadel Group Limited
CGL subsidiary companies and business partners	• Australian Business Academy • filosoph-e • Frontier People • Jakeman Business Solutions • PJA Solutions • ServicePoint Australia • SME Gateway
DEEWR	Department of Education, Employment and Workplace Relations
DISP	Defence Industry Security Program
OAIC	Office of Australian Information Commissioner

1.2 PURPOSE (WHY WE NEED TO DO IT)

The **Australian Privacy Principles** (APP) covers the collection, use, disclosure and storage of personal information. They allow individuals to access their personal information and have it corrected if it is incorrect. There are also separate APPs that deal with the use and disclosure of personal information for the purpose of direct marketing (APP 7); cross-border disclosure of personal information (APP 8); and the adoption, use and disclosure of government-related identifiers (APP 9).

1.3 REPORTING

1.3.1 Roles and Responsibilities

Privacy is a shared responsibility and all CGL leaders and managers are responsible for implementing this GOV 600 CGL Privacy Policy. Appointed Privacy Officers are responsible for providing advice on privacy management issues which, ultimately, reside with CGL Managing Director. However, authority and responsibility for the management and use of personal information is delegated and assigned at all levels.

In the first instance, a person can request access to their personal information by contacting the nominated Privacy Officer(s) the CGL Managing Director or the ABA General Manager:

	CGL Privacy Officer	**ABA Privacy Officer (Students)**
By Post	Managing Director, The Citadel Group Citadel House, High Technology Park, Level 1, 11-13 Faulding St, Symonston ACT 2609	General Manager, The Australian Business Academy Citadel House, High Technology Park, Level 1, 11-13 Faulding St, Symonston ACT 2609
By Phone	(02) 6124 0800	(02) 6124 0800
By Email	Miles.Jakeman@citadelgroup.com.au	Andrew.Pike@aba.edu.com

1.4 SCOPE (WHAT'S INVOLVED)

1.4.1 Why we collect, hold, use and disclose personal information

CGL is one of Australia's leading professional and managed service providers with over 200 staff nationwide, a $50 million annual turnover, and an ability to 'reach back' and draw on the expertise of over 3,000 people. CGL's client base includes government agencies at all three levels - i.e. local, state and federal - as well as blue chip private sector businesses. CGL is represented on over 200 different contract and panel arrangements nationally, many of them established organisations seeking specialist skills to deliver successful programs. CGL operates through semi-autonomous, individually branded and trading businesses that provide a breadth and depth of capability with a portfolio of specialised professional and managed service solutions:

Australian Business Academy Pty Ltd (ABA) – training services and solutions as a Registered Training Organisation

Frontier Group Australia Pty Ltd (Frontier People) – HR and recruitment solutions

Jakeman Business Solutions Pty Ltd (JBS) - consulting and contract support services, and Registered Training Organisation.

PJA Solutions specialises in creating and supporting software products for diagnostic laboratories and clinical applications in public hospitals as well as public health and forensic sciences laboratories.

ServicePoint Australia Pty Ltd (ServicePoint) – integrated communication services

CGL and its subsidiary companies also own shareholdings in:

filosoph-e Pty Ltd – fully managed services for the Department of Defence

SME Gateway Limited –engineering and professional services.

Briefly, our activities and services include:

- **Professional Services** to a broad range of large Australian enterprises and Government, with particular focus on assisting clients to optimise their activities. These include effective programme management, risk management, acquisition and sustainment advice, planning and quality assurance, software and systems integration, and aftermarket support services.
- **Managed Solutions** providing tailored implementation, integration and application support services to enterprises and government departments across Australia and the Asia-Pacific.
- **Training Services** delivering both nationally accredited vocational training (Certificate through to Advanced Diploma level courses) and non-accredited professional development training to clients.

1.4.2 Australian Privacy Principles Quick Reference

Consideration of Personal Information

1. **Open and transparent management of personal information:** Ensures that CGL manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

2. **Anonymity and pseudonymity:** Requires CGL to give individuals the option of not identifying themselves, or of using a pseudonym where appropriate. Exceptions apply, such as when information is required to deal with government agencies.

Collection of Personal Information

3. **Collection of solicited personal information:** Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

4. **Dealing with unsolicited personal information:** Outlines how CGL must deal with unsolicited personal information.

5. **Notification of the collection of personal information:** Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

Dealing with Personal Information

6. **Use or disclosure of personal information:** Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

7. **Direct marketing:** An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

8. **Cross-border disclosure of personal information:** Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

9. **Adoption, use or disclosure of government related identifiers:** Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Integrity of Personal Information

10. **Quality of personal information:** An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

11. **Security of personal information:** An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

Access to, and Correction of, Personal Information

12. **Access to personal information:** Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

13. **Correction of personal information:** Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

1.5 PRACTICE (HOW WE DO IT)

1.5.1 The kinds of personal information

In undertaking CGL activities, we collect personal information based on the nature of the relationship, activity or service. It may include (but is not limited to) a person's name, contact details, date of birth, occupation, family background and financial records.

We may hold sensitive personal information about employees, associates or students. This may include information about health, disability, racial or ethnic origin, education, criminal convictions, personnel files, external salary deductions or payments, bank accounts, complaints, appeals, employment histories, external requests from government bodies, academic assessment results and tax file numbers.

This information is collected with consideration on the restrictions placed when collecting sensitive personal information about persons. CGL may collect sensitive information when:

- it is required to provide specific services (for example, managing graduated return to work)
- assessing eligibility for employment or course participation (for example, potential or existing employees or students);
- for the purpose of maintaining the employee/employer relationship (for example, formal or informal employee feedback, employee pay information);
- advising on health services to persons (for example, to an employee or student experiencing personal difficulties); and,
- for the purpose of meeting legal obligations (for example, reporting of student information to government agencies).

Where CGL conducts online collaboration, social media or market research, it may also ask for public opinions about its services or staff. CGL will treat these opinions as personal information in accordance with the APPs if they contain personally identifiable information.

1.5.2 How we collect and hold personal information

If it is reasonable and practical to do so, CGL will collect personal information directly from the persons concerned with their consent. This may be through application forms, over the telephone, the Internet, or in person. We may also need to collect personal information from other people or organisations. This information is collected with the person's consent, except in circumstances allowed for by legislation. Sometimes this may happen without direct involvement. Some examples of the people or organisations from which CGL may collect personal information about persons are:

- clients or customers;
- publicly available sources of information (such as telephone directories);
- person's representatives (such as a parent/guardian, managers, teachers, assessors, legal adviser);
- person's employers;
- government agencies; and,
- law enforcement agencies.

So that CGL can better tailor information and services to individual needs, when it sends email messages, it may use technology to identify persons to know when email is opened or links used within an email.

If persons log into or use CGL company assets such as intranet, internet, phones, etc information will be collected from them to confirm their identity.

CGL will hold the information it collects on electronic systems and, where appropriate, in paper format. If required, such as for student information, these holdings will be consistent with government archival standards or legislation.

CGL may also hold or receive some information on cloud-based systems. Where this occurs, the relevant service will have been subject to a CGL risk assessment and be compliant with the privacy and security standards required by CGL in protecting personal information.

1.5.3 When we will not need to collect personal information

Depending on the nature of a person's relationship with CGL, they may not need to identify themselves personally as they have a right to pseudonymity or anonymity when dealing with CGL, unless:

- CGL is required or authorised by or under an Australian law, or a court/tribunal order to deal with individuals who have identified themselves;

- it is impracticable to deal with individuals who have not identified themselves; and,
- the person is receiving a service or financial benefit from CGL, which necessitates assurance that the service or money is being directed to an identified person.

1.5.4 How CGL will keep personal information accurate and up-to-date

CGL seeks to maintain the quality of its information holdings by taking reasonable administrative and technical steps to make sure that the information collected, used and disclosed is accurate, complete and up-to-date.

1.5.5 How CGL will keep information and data secure

CGL utilises up-to-date techniques and processes, which meet current government requirements including security arrangements, to protect personal information from misuse, loss and unauthorised access, modification or disclosure.

Paper documents are protected from unauthorised access or use through the various security systems that we have over our physical premises. We also maintain up-to-date computer and network security systems with appropriate firewalls, access controls and passwords to protect electronic copies of personal information.

The only people permitted to handle or have access to personal information are CGL staff and those who perform services for CGL who need such personal information to do their jobs. All CGL staff are bound by the CGL *c*ode of conduct not to misuse personal information, and privacy clauses are included in all agreements with employees and independent contractors who perform services on CGL's behalf.

If we no longer require an individual's personal information, we will take reasonable steps to destroy it in a secure manner or remove identifying features from it. This is subject to any legal obligation (such as the *Archives Act, 1983*) that requires CGL or its subsidiaries to keep information for a certain period of time.

1.5.6 Circumstances where CGL may provide personal information to others

CGL strives to limit the information it provides to outside organisations to what they need to provide their services to us - or to provide services to CGL clients, customers or students. CGL ensures that any organisation that it contracts with:

- meet the privacy standards required by CGL in protecting personal information and complies with the *Privacy Act 1988*; and
- use the personal information provided only for the purposes of the specific service being provided to CGL, and for no other purpose.

Sometimes CGL may be required to provide personal information to external organisations. Generally, these organisations help CGL conduct its programs and activities. These organisations may include but are not limited:

- business partners (organisations with whom we have agreements to provide products or services);
- authorised representatives of CGL;
- superannuation funds;
- payment systems operators (for example, online for credit card payments)
- comply with commonwealth reporting requirements (for example, ASQA for quality indicator information, or DEEWR on the status of overseas students);
- personal information in support of security clearance obligations under DISP; or,
- our accountants, auditors or lawyers;
- cloud-based services that host CGL data on its servers; and
- person's representative(s).

CGL may also need to provide personal information to others outside CGL where:

- legally bound to do so or has a public duty to do so. For example, a Court, a regulator (such as the Australian Taxation Office, Fair Work Australia, ASQA or the police); and
- persons have expressly consented to their personal information being supplied to others for particular purposes.

1.5.7 Disclosure of personal information to overseas recipients

CGL seeks to limit where possible the disclosure of personal information to overseas recipients. These requests for personal information will be dealt with by the relevant Privacy Officer and in accordance with the APP. Instances where this may arise include but are not limited to:

- information provided in the management of travel or logistics for CGL staff members engaged via government contracts particularly with regard to security arrangements;
- the information is provided in the management or administration of overseas students, particularly those under the age of 18; and,
- a person has expressly consented to their personal information being supplied to overseas recipients.

From time-to-time CGL may contract overseas commercial organisations to provide products or services to CGL or its clients. These agreements are entered into where:

- CGL has conducted a risk assessment;
- the organisation meets the privacy and security standards required by CGL in protecting personal information; and,
- the organisation uses personal information only for the specific service CGL asks them to provide, and for no other purpose.

1.5.8 Access and correction to personal information held by CGL

Any person who believes that CGL holds personal information about them may contact us to seek access to that information. If after accessing information held and the person considers that it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purposes for which it is held, then they may make a request in writing to the CGL Privacy Office to amend it in accordance with APP 13.

CGL may not always be able to provide access to all the personal information it holds about a person. For example, it may not be able to provide access to information that would reveal personal information about another person. Any person may also obtain access to their personal information held by CGL through the *Privacy Act 1988* and the *Freedom of Information Act 1982*.

1.5.9 Complaints

CGL will be efficient and fair when investigating and responding to any privacy complaint in accordance with the guidelines published by the OAIC. Any privacy complaints received by CGL must be in writing and will be initially investigated by the nominated CGL Privacy Officer. If required, escalated is to the CGL Managing Director. CGL will respond to all complaints within a reasonable time period appropriate to the specific complaint.

Any person may also complain to the OAIC who may investigate CGL's actions. The Commonwealth Ombudsman may also investigate complaints about CGL actions. However, the Commonwealth Ombudsman and the Privacy Commissioner will consult to avoid the same matter being investigated twice.

2 APPENDIX 1: AUSTRALIAN PRIVACY PRINCIPLES FACT SHEET

This appendix provides 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.

2.1 PART 1—CONSIDERATION OF PERSONAL INFORMATION PRIVACY

2.1.1 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.

2.1.2 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.

2.2 PART 2—COLLECTION OF PERSONAL INFORMATION

2.2.1 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.3

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.

2.2.2 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.

2.2.3 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 4 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.

2.3 PART 3—DEALING WITH PERSONAL INFORMATION

2.3.1 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; or5

(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.

2.3.2 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.6 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.

2.3.3 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.8

2.3.4 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).

2.4 PART 4—INTEGRITY OF PERSONAL INFORMATION

2.4.1 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.

2.4.2 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:9

(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.

2.5 PART 5—ACCESS TO, AND CORRECTION OF, PERSONAL INFORMATION

2.5.1 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;

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; or10

(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.

2.5.2 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:

(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) 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).

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice. For further information telephone: 1300 363 992 email: enquiries@oaic.gov.au write: GPO Box 5218, Sydney NSW 2001 GPO Box 2999, Canberra ACT 2601 or visit our website at www.oaic.gov.au

The Citadel Group Limited

ACN 127 151 026

Citadel House | High Technology Park

11-13 Faulding Street | Symonston | ACT | 2609

T: 02 6124 0800 | www.citadelgroup.com.au