Privacy and Confidentiality Policy and Procedure

Belconnen Community Service Inc (BCS) is committed to ensuring the privacy of an individual's information.

BCS is bound by the Privacy Act 1988 and will ensure that an individual's privacy is maintained through the correct collection, use, storage, security and disclosure, in accordance with the Australian Privacy Principles (APP). BCS aims to protect the rights of individuals to access and control what happens with any and all of their personal information provided to the organisation.

Employees and volunteers of BCS are required to comply with this policy and procedure and any legal obligation in relation to the collection, use, storage, security and disclosure of an individual's personal information.

All employees and volunteers of BCS are required to maintain the confidentiality of all information, records, discussions and documentation in relation to service recipients, employees, volunteers, contractors, consultants financial, contractual arrangements and external stakeholders. All employees and volunteers must sign a confidentiality agreement as a condition of employment/engagement with BCS.

Employees or volunteers who breach this policy and procedure or legal obligation will face disciplinary action up to and including termination.

Scope

This Policy and Procedure is relevant to all information in relation to individuals who are:

- recipients of service by BCS (such as participants, child care recipients and families, etc)
- prospective employees, volunteers or other individuals who seek to be engaged in any work capacity by BCS
- employed or engaged directly by BCS, (such as employees; volunteers; agency staff; and other specified personnel directly engaged by BCS, such as, students, consultants, contractors and allied professionals)

BCS will keep records relevant to this policy and procedure in relation to:

- service recipient personal information,
- details of contact with the service recipient (child observation, one to one client sessions),
- details of incident reports which may involve service recipients,
- details of financial and commercial transactions,
- applications for employment/engagement and pre-employment/engagement checks,
- contractor personal information
- AFP National Police Checks for employment/engagement purposes,
- payroll and personnel details (including relevant superannuation, banking and tax file number information),

- the employment/engagement relationship (all documents relating to the day to day working relationship e.g. performance reviews, disciplinary measures, contracts of employments/engagement, applications, reference reports etc.),
- any workers compensation or relevant functional assessment or medical information relating to the employment/engagement relationship, and
- incident reports, investigations and other documentation in relation to the safety and well being of employees, volunteers, service recipients and visitors.

Definitions

Australian Privacy Principles:	**a single set of principles from the Legislation that apply to both agencies and organisations. See attachment B for a summary list of the APPs sourced from the Office of the Australian Information Commissioner**
Cross Border	**relates to national borders. When information crosses borders it is given to an overseas recipient.**
Personal Information:	Information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. **Examples of Personal Information can include:** • Name and address • Name and Licence details • Bank account details • Communications with others • Photo's • Video's • Information about what you like • Your opinions • Where you work. • Sensitive information
Sensitive Information:	Information or an opinion about an individual which includes: • Racial or ethnic origin • Political opinion • Membership of a political association • Religious beliefs

- Philosophical belief
- Membership of a professional or trade association
- Membership of a trade union
- Sexual preference or practices
- Criminal record
- Health information

Identifier: Includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. An individual's name is NOT an identifier for the purposes of this Policy and Procedure and the Privacy Act 1988 (*the Act*).

Confidential Information: Includes:

- all service user information (in particular personal and sensitive information),
- employee, volunteer, contractor or consultant personal information, payroll, employment, remuneration, disciplinary or performance information,
- Workers Compensations claims,
- BCS financial information,
- contractual agreements,
- recruitment information including applicant names, referee reports, interview notes and pre-employment assessments,
- AFP National Police Checks, and
- any other information that BCS owns or relies on in the operation of the organisation that is not public knowledge.

PROCEDURE

BCS will protect the privacy of individuals in accordance with the Australian Privacy Principles as outlined within the Privacy Act 1988. In order to ensure the privacy of individuals, this procedure outlines the requirements in relation to:

1. The collection of personal information
2. Use and disclosure
3. Data quality
4. Data Security

5. Openness
6. Access and correction
7. Identifiers
8. Anonymity
9. Transborder data flows
10. Sensitive Information
11. Personnel Records
12. Privacy Complaints
13. Confidentiality

1. The Collection of Personal Information

Personal information in relation to service recipients and prospective employees and volunteers can only be collected when it is necessary for a service's activities. The information must be needed for the provision of services.

1.1. Personal information must be collected with the individual's consent.

1.2. Questions cannot be asked nor information gained just for personal interest, nor can they be gained for a purpose that has not been disclosed to the individual.

1.3. Only lawful and fair means must be used to collect information.

1.4. Personal information can only be collected directly from an individual when it is reasonable and practical to do so, and is not unduly inconveniencing the individual.

1.5. At the time the personal information is being collected the individual must be given a collection notice (samples at attachment A) that consists of:

1.5.1. The name of the service and how to contact the service.

1.5.2. How they access the information held about them.

1.5.3. Why the service or employee is collecting this information about them.

1.5.4. How the information will be used or disclosed.

1.5.5. Any law regarding the collection of the information and the consequences of not providing the information.

1.5.6. The complaint process

1.6. Information will only be collected from a third party when:

1.6.1 consent is given

1.6.2 it is unreasonable and/or impracticable to collect the information from the individual

1.7. Even if an individual's personal information is collected from a third party the individual must still be made aware of all the information in 1.5.

2. Use and Disclosure

Information relating to service recipients and prospective employees or volunteers can only be used or disclosed for its original purpose of collection.

2.1 Individuals about who personal information is kept should be informed that:

- 2.1.1 information is being kept and the purpose for which it is being kept,
- 2.1.2 the nature of the information,
- 2.1.3 the information is available to them upon request, and
- 2.1.4 the information will not be disclosed to any other person without their knowledge unless there is a legal requirement to do so.

2.2 When information is collected indirectly, BCS must check with the individual to ensure that they have agreed to hand over the information to BCS. A signed authority by the individual to provide information to BCS will be considered authority to accept the information.

2.3 BCS may use de-identified information for evaluation and to meet performance standards.

2.4 Individuals who are service users or prospective employees or volunteers may withdraw consent to release of personal information at any time.

2.5 Recipients of direct marketing must have given their consent to be included on the mailing list and be given opportunity to opt out of receiving further correspondence. Examples of direct marketing include but are not limited to promotion emails and bulk mailouts. Recipients must be provided with the ability to cancel and stop receiving further direct marketing communications.

2.6 Information will only be used or disclosed for other or secondary purposes when:

- 2.6.1 The individual has consented to its use for a secondary purpose;
- 2.6.2 The secondary purpose is related to the primary purpose and the individual would reasonably expect the service or worker to use or disclose the information for that secondary purpose;
- 2.6.3 If the information is sensitive it needs to be directly related to the primary purpose
- 2.6.4 Information given indicates potential or intent to harm others or self or commit a criminal act;
- 2.6.5 Information given results in the disclosure of a child protection issue (see Child Protection policy);
- 2.6.6 The use or disclosure is required by law.
- 2.6.7 Permitted general situations for a secondary purpose is allowed if:
  - 2.6.7.1 BCS has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the agency's functions or activities has been, is being, or may be engaged in, and the BCS reasonably believes that the use or disclosure is necessary in order for it to take appropriate action in relation to the matter
  - 2.6.7.2 BCS reasonably believes it necessary to assist any APP entity to locate a missing person and the use of disclosure complies with rules made by the Commissioner

2.6.7.3 Reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.

2.6.7.4 Reasonably necessary for the purpose of a confidential alternative dispute resolution process.

2.7 If disclosure of personal information is necessary the worker must make a written note of such a disclosure.

3. Data Quality

All information must be recorded without bias, feeling, assumption and undue subjectivity.

3.1 Services must ensure all information collected and held is accurate, relevant, complete and up-to-date.

3.2 The employee recording the personal information should always be identifiable on the record.

3.3 Should there be a requirement to pass on information to a third party, BCS will check the information held is accurate, relevant, complete and up to date before handover wherever practicable.

3.4 As a minimum records will be reviewed for updates every 6 months.

4. Data Security

BCS will take reasonable precautions to protect personal information so that it is not misused, lost, accessed by unauthorised people, modified or disclosed.

4.1 Filing cabinets containing personal and sensitive information need to be locked when not in use, and keys to these filing cabinets held only by relevant authorised employees.

4.2 Files and information should be filed away when not in use, and should never be left on desks or in areas where other people can read or access it.

4.3 Where 4.1 and/or 4.2 above are not feasible, a risk assessment is to be completed. Offices and rooms with personal and sensitive information should be locked when not occupied.

4.4 Access by employees or volunteers to personal information will be on a “need to know” basis only.

4.5 Unauthorised access or disclosure of personal information will result in disciplinary action

4.6 Computers that store, or can access other computers that store personal information must have password protection.

4.7 Each computer user must have a password. Passwords must not be shared. Access must only be provided to users who are required to have the information in order to undertake their role For further information see ICT Policy

4.8 Archive areas must be secured.

4.9 Proper records of where files are archived must be held.

4.10 All personal and sensitive information should be securely destroyed or de-identified when no longer needed or statutory times for holding have passed. Personal and sensitive information must never be disposed of by general disposal methods.

4.11 Reasonable steps must be taken to destroy or de-identify personal information that is no longer needed.

4.12 Practices of security will be monitored to ensure compliance with policies.

5. Openness

5.1 BCS will ensure that all individuals will have access to this policy and procedure upon request.

5.2 Individuals will be informed of:

5.2.1 what sort of personal information BCS holds,

5.2.2 for what purpose,

5.2.3 how BCS collects the information,

5.2.4 how BCS holds the information,

5.2.5 how BCS uses the information, and

5.2.6 how BCS discloses the information.

5.2.7 how to make a complaint

6. Access and Correction

6.1 Where BCS holds personal information about an individual, BCS will provide the individual with access to the information upon written request within 14 days where practicable.

6.2 The file is and remains the property of BCS and should only leave the service under subpoena by a court.

6.3 All information provided or entries made in an individual's file must be signed by the source. It is the responsibility of service coordinators to preserve the security of written records.

6.4 The coordinator/program manager shall be notified prior to an individual gaining access to any file.

6.5 The coordinator/program manager shall be present to assist the individual when accessing information in his/her file.

6.6 Access to information will only be denied where:

6.7 BCS is authorised to refuse under FOI or another Commonwealth Act

6.8 access would pose a serious and imminent threat to the life or health of any individual,

6.9 access would have an unreasonable impact of the privacy of other individuals,

6.10 access is considered vexatious or frivolous,

6.10.1 the information related to existing or anticipated legal proceedings and the information would not be accessible by the process of discovery in those proceedings,

6.10.2 providing access would be unlawful,

6.10.3 providing access would be likely to prejudice an investigation of possible unlawful activity, or

6.10.4 other areas as specified by the Privacy Act 1988.

6.11 If an individual requests that information relating to them, or if BCS establishes that information held by BCS is not accurate, complete, up-to-date, relevant or is misleading, BCS will take all reasonable steps to correct the information so that it is accurate, complete, up-to-date, relevant and not misleading.

6.12 If the individual and BCS disagree about whether the information BCS holds is accurate, complete and up-to-date, BCS will store with the information a statement from the individual outlining their view in relation to the accuracy, completion and updated information

6.13 BCS will provide an individual with a reason in writing (including the complaints mechanism) if access to information has been denied or the manner requested to access has been denied or BCS has refused to correct personal information. If BCS has denied the request on the basis of the requested manner in which access was requested, BCS will take reasonable steps to provide access in a way that meets both BCS and the individual's needs.

7. Identifiers

7.1 Where BCS uses a system to identify individuals other than their name, BCS will not use:

7.1.1 a Commonwealth Government identifier, or

7.1.2 an identifier that has been assigned by an agency or an agent of an agency.

7.2 BCS will not use or disclose an identifier assigned to an individual by an agency or by an agent of an agency unless:

7.2.1 the use or disclosure is necessary for BCS to fulfil its obligations to the agency,

7.2.2 BCS reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety,

7.2.3 BCS has reason to suspect that unlawful activity has been, is being, or may be engaged in; and uses or discloses the identifier as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

7.2.4 The use or disclosure is required by law.

8. Anonymity

8.1 In circumstances where it is lawful and practicable participants will be given the option of interacting anonymously with BCS.

8.2 In BCS children's programs and services anonymity is not possible as they require contact details for duty of care purposes.

8.3 If an individual prefers to interact anonymously with BCS the individual will be given an identifier for record keeping purposes. For example “Mary Smith C/- BCS”

9. Trans border Data Flows

9.1 BCS will not transfer personal information about an individual overseas except where:

9.1.1 the individual has provided consent,

9.1.2 the recipient of the information is required, by law or a binding scheme, to protect the information similar to the APPs and that the individual to whom the information relates is able to enforce these protections

9.1.3 the transfer is necessary for the performance of a contract between the individual and BCS,

9.1.4 the transfer is required by an Australian law or court/tribunal order

9.1.5 the transfer is for the benefit of the individual, and it is impractical to obtain consent from the individual and it is likely that the individual would agree to the transfer of information.

9.1.6 An individual consents to cross border disclosure after BCS expressly informs them in writing that BCS **cannot** ensure that the overseas recipient of the information will not breach the APP’s. Furthermore, as BCS has expressly informed the individual of this situation, giving their consent will mean the APPs will not apply to the overseas recipient of the information and the individual’s privacy cannot be guaranteed..

9.1.7 A permitted general situation exists, other than disclosure, for the established exercise or defence of a legal or equitable claim, or for the purposes of a confidential alternative dispute resolution process.

9.1.8 Disclosure of info required under an international agreement relating to info sharing to which Australia is a party

9.1.9 BCS reasonably believes that the disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, and the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body

10. Sensitive Information

10.1 BCS will only collect sensitive information if:

10.1.1 the information is required in order to provide a service,

10.1.2 the individual consents,

10.1.3 the collection is required by law,

10.1.4 the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual where the individual who the information concerns:

10.1.4.1 is physically or legally incapable of giving consent to the collection; or

10.1.4.2 physically cannot communicate consent, and

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

11. Personnel Records

11.1 Whilst records held by BCS in relation to the employment/engagement relationship (such as personnel and payroll files) do not fall under the coverage of the Privacy Act 1988, BCS will ensure that all records relating to employees and volunteers are held in the strictest of confidence.

11.2 A personnel file and a payroll file will be created for all employees and volunteers at the commencement of their employment/engagement, and maintained throughout their period of employment/engagement.

11.3 Employee and volunteer personnel and payroll information will be stored in locked filing cabinets within the People and Culture department.

11.5 Only BCS employees who are required to access personnel or payroll files in order to undertake their job will have access to personnel files. These BCS employees are limited to:

11.3.1 Chief Executive Officer (all access)

11.3.2 Executive Manager - People and Culture (all access)

11.3.3 People and Culture employees (limited access)

11.6 Executive Managers and line managers can access information in relation to employees and volunteers within their program or service. A line manager can only access files of employees or volunteers who report directly or indirectly to them. Executive Managers and line managers can only access personnel files upon request to the Executive Manager - People and Culture. Files cannot be removed from the People and Culture department and remain the property of BCS.

11.7 Information will only be disclosed to third parties where:

11.7.1 the employee or volunteer authorises the disclosure,

11.7.2 BCS is required by law, or

11.7.3 identifying information has been removed for statistical or research purposes.

11.8 Personnel files shall as a minimum contain the following:

11.8.1 Applications for employment/engagement and written references provided to and by BCS.

11.8.2 Resume or CV.

11.8.3 Results of employment screening checks.

11.8.4 Written acceptance of the initial offer of employment/engagement and any variations.

11.8.5 Position descriptions.

11.8.6 Evidence of qualifications.

11.8.7 Performance Management reports.

11.8.8 Written understanding and acceptance of BCS policy, procedures and guidelines.

11.8.9 On departure - letter of resignation or dismissal.

11.8.10 Any disciplinary warnings.

11.9 Payroll files shall contain the following:

11.9.1 Written acceptance of the initial offer of employment and subsequent changes to that offer.

11.9.2 Position title and classification of the employee and the relevant award, where applicable.

11.9.3 The number of hours worked each week.

11.9.4 The rate at which the employee is paid and banking details.

11.9.5 Tax Declaration forms.

11.9.6 Leave records.

11.9.7 The amount of wages paid to the employee showing deductions from such wages.

11.9.8 Copy of documentation regarding changes in salary and conditions.

11.9.9 Other particulars that would show on an inspection of the records that the wages and hours provisions of the award or agreement have been complied with.

11.10 Employees and volunteers may only access their Personnel file in the presence of a member of People and Culture

11.11 Employees may contact the Executive Manager - People and Culture in writing to request access to their payroll and/or personnel files at any time. The Executive Manager - People and Culture will organise a suitable time for this access.

11.12 Employees must have the Payroll Officer or Executive Manager - People and Culture present when viewing their Payroll file.

11.13 Employees have the opportunity to attach statements to their Personnel file.

11.14 Following the departure of an employee or volunteer, their Personnel and Payroll files are to be kept for a period of ten years and shall be accessible only to the relevant supervisor, manager, executive manager, People and Culture personnel and Chief Executive Officer.

12. Privacy Complaints

12.1 An individual has a right to make a complaint about their treatment in regards to any part of the BCS privacy policy and procedures.

12.2 Service recipients can lodge their complaint in writing to:

ATT: Chief Executive Officer
Belconnen Community Service Inc.
PO Box 679
BELCONNEN ACT 2616

or via email to *Dira.Horne@bcsact.com.au*

12.3 Complaints will be dealt with In accordance with the BCS Feedback Policy and Procedure. Alternatively complaints can be lodged directly with the Privacy Commissioner:

The Privacy Commissioner
GPO Box 5218

SYDNEY NSW 2001

Privacy Hotline:1300 363 992

Further information: *www.privacy.gov.au*

12.4 Employees and Volunteers can lodge a grievance in accordance with the BCS Grievance and Dispute Handling Policy. For further information contact the People and Culture on 02 6264 0200.

13. Confidentiality Requirements of Employees and Volunteers

13.1 Employees and volunteers who have access to or knowledge of confidential information during the course of their employment with BCS must not:

13.1.1 use this confidential information for his/her own purposes, or

13.1.2 discuss with any third party, or

13.1.3 disclose the information to any external party or future employer.

13.2 Confidential information is the exclusive property of BCS.

13.3 BCS requires that employees and volunteers do not:

13.3.1 Solicit customers and/or erode goodwill;

13.3.2 use or disclose information without authorisation;

13.3.3 comment on BCS business without authorisation;

13.3.4 accept or offer bribes and secret commissions;

13.4 Employees and volunteers must not, except in the proper course of their duties or as permitted by BCS or as required by law, divulge to any person any confidential information concerning:

13.4.1 service recipient information;

13.4.2 the business or financial arrangements or position of BCS;

13.4.3 any of the dealings, transactions or affairs of BCS, or

13.4.4 employee, volunteer, consultant or contractor information.

13.5 Employees and volunteers must not knowingly access any confidential information about BCS service recipients, employees/volunteers or financial operations, unless such information is essential for the individual to properly and efficiently perform their duties.

13.6 Employees and volunteers must not initiate or participate in unnecessary discussion or gossip of confidential information to another individual. Any employee or volunteer who has been found to have breached this policy and procedure will face disciplinary action up to and including termination and/or civil proceedings.

13.7 All employees and volunteers must inform their supervisor immediately if they become aware of any breach of privacy or security in the course of their duties.

13.8 This restriction ceases to apply to any information or knowledge, which subsequently comes into the public domain by way of authorised disclosure.

13.9 All confidential records, documents and other papers together with any copies or extracts thereof in an employee or volunteer's possession must be returned to BCS on the termination of the individual's employment/engagement.

Relevant Legislation, Resources and BCS Policies

- *Privacy Act 1988*
- *13 Australian Privacy Principles - http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles*
- *Belconnen Community Services*
  - Code of Conduct
  - *BCS Feedback Policy*
  - *BCS Grievance and Dispute Handling Policy*

Acknowledgement / Sources

- *www.privacy.gov.au*
- *www.oaic.gov.au*

Feedback

Feedback on this policy can be submitted by email to policy@bcsact.com.au.

Review

This policy will be reviewed within 3 years.

Compliance

Non-compliance to this policy may result in disciplinary action up to and including dismissal.

***ATTACHMENT A - Sample Collection Notices**:*

Replace the *italic brown words* with appropriate details for your program.

Verbal

I need to let you know you are talking to the BCS *Children's Services Admin Team* and we can be contacted by either calling this number or the BCS central phone number 62640200. The information we collect today will be used to *identify a place for your your child in one of our long day care centres*, without this information we will be unable to offer *you care for your child*. Your details will be disclosed to *the BCS childcare service when your child is offered a place*. If you are unsatisfied with our service you can email our feedback address which is feedback@bcsact.com.au.

***Written* –** *Where BCS, program and contact details are Identified on document*:

The information collected on this form/document/email will be used for/to *identify a place for your child in the Evatt Kids Club*. BCS is required to collect this information by (any laws/regs etc if no specific laws/regulations etc omit this sentence)*No laws requiring this information for SAC therefore this sentence would be omitted*. Without this information BCS/program will be unable to *provide After School Care for your child*. To update, remove or access your personal information contact us either by email *csat@bcsact.com.au* or phoning *62640200*. Your details will be used/disclosed for/to the Director of Evatt Kid's Club when a position becomes available. If you are unsatisfied with our service you can email our feedback address which is feedback@bcsact.com.au.

***Written* –** *Where BCS and program are not Identified*:

Home and Community Care is a Belconnen Community Service (BCS) program, we can be contacted by either calling *627881??* (or program number) or the BCS central phone number 62640200.The information collected on this form/document/email will be used for/to *provide you with the requested service of personal care*. BCS is required to collect this information by (any laws/regs etc if no specific laws/regulations etc omit this sentence) *If regulations require certain information to be collected add them here otherwise delete this sentence*. Without this information the *BCS Home and Community Care P*rogram would be unable to *provide this service*. To update, remove or access your personal information we can be contacted either by email *programemail@bcsact.com.au* (Program Email), or on the above phone numbers. Your details will be used/disclosed for/to *our employees providing the care, add any other place the program may need to report a participants individual details to*. If you are unsatisfied with our service you can email the BCS feedback address feedback@bcsact.com.au.

ATTACHMENT B: Overview of Australian Privacy Principles

Sourced from: Office of the Australian Information Commissioner

Australian Privacy Principles — a summary for APP entities

from 12 March 2014

Australian Government
Office of the Australian Information Commissioner

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 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.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 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.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

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

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 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.

APP 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.

APP 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.

APP 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.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

For private sector organisations, Australian Government and Norfolk Island agencies covered by the *Privacy Act 1988*

www.oaic.gov.au