Guide to the Access and Issue of "Forgotten Australians" Client Records (records pre 1989)

This Guide was developed on behalf of Lentara UnitingCare by Mimi Morizzi, Primex Records Management with financial contributions from Lentara UnitingCare and UnitingCare Victoria and Tasmania.

Table of Contents

Document Control	
Title	Guide to the Access and Issue of "Forgotten Australian" Client Records (records pre 1989)
Version	3
Document Owner	Lentara UnitingCare
Release Date	3 April 2014

1.0 Introduction

This Guide has been produced to assist with a broader process of service provision for people collectively identified by the Australian Senate Community Services References Committee as "Forgotten Australians" – people who grew up in out-of-home or institutional care. In considering services for Forgotten Australians, many having a long association with the Uniting Church in Australia, the following guiding principles were determined:

- The welfare and interests of the care leavers, their families and those we serve are paramount and our services will be delivered sensitively, compassionately and with respect.
- In consultation with the people we serve, we will undertake effective intervention in the least intrusive manner so as to achieve the most favourable outcome in service delivery and to prevent any harm or distress.
- We will provide services that are accessible, inclusive and culturally competent
- We will work with our community to promote and achieve social justice and economic parities that support the poor and marginalised.

The Child and Family Welfare sector has become heavily regulated following changes to laws governing information privacy, evidence and legal discovery. To this extent, this Guide is also an evolving instrument that will require updating to reflect both legislative changes and community expectations. Hence the previous version of this Guide (Version 2) has being reviewed and updated post the introduction of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (effective 12 March 2014) containing 13 new Australian Privacy Principles (APP's) that replace the National Privacy Principles.

Notwithstanding the regulatory impositions to providing records access, Community Service Organisations (CSOs) are encouraged to "open the archives" and assist our clients, particularly care leavers, to obtain as much information about themselves, their families and their time in care as possible. A good starting point when administering access is to ask oneself "Why shouldn't I provide this information?" rather than "Why should I provide this information?" – noting that Privacy laws are enabling legislations.

This Guide specifies the current regulatory access provisions applying to pre 1989 records of institutional and out-of-home care of children as held in CSOs. For more contemporary client records, that is, records post 1989; the CSO will need to refer to their in-house Privacy Policy and administer access to those records accordingly, taking into consideration any records management instruction provided in contracts by funding providers.

The information provided in this Guide is for reference only and CSOs should consult their legal advisers to confirm that statutory requirements are being met. Additionally, this Guide does not seek to include consideration of intellectual property rights when administering access as this area of law would require a guide in itself; however, it is prudent to consider intellectual property rights when providing access to records such as photographs.

In brief, photographs held by a CSO that were taken pre 1 January 1955 are out of copyright and considered to be information in the public domain. For photographs which were still in copyright on 1 January 1995, or which were created on or after that date, copyright is 70 years from the end of the year the photographer died. A photographer is generally the owner of copyright however, there are some exceptions - copyright in a photograph taken during the course of a person's employment will be owned by that person's employer, unless there is an express or implied agreement that the employee will own the copyright.

1.1 The Legislative Framework Governing Privacy

The following legislation has direct bearing on the way we currently provide access to client records held by CSOs that have provided residential care for children. It is imperative that staff have a working knowledge of the following legislation if we are to manage information so as to (a) ensure compliance with legislation; (b) make informed decisions; (c) provide quality services to our clients; (d) provide evidence of our business transactions; and (e) minimise organisational and personal risk.

Special note: while some legislation has limited application prior to the year 2001, the intent of this Guide is to use the legislation as best practice for guiding how access is to be administered.

Pursuant to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* effective 12 March 2014, the primary Acts that regulate the privacy of information within a CSO are:

- ***Privacy Act 1988 (Commonwealth)***
- ***Health Records Act 2001 (Vic)****; and*
- ***Adoption Act 1984 (Vic)***

Other relevant Acts that regulate access to information within a CSO include the following:

- ***Evidence (Document Unavailability) Act 2006 (Vic)***
- ***Evidence (Miscellaneous Provisions) Act 1958 (Vic)***
- ***Evidence Act 2008 (Vic)***
- ***Crimes Act 1958, Part 1, Division 5***
- ***Civil Procedure Act 2010***
- ***Electronic Transactions (Victoria) Act 2000,***

Some key points of those Acts most relevant are listed below:

Privacy Act 1988 (Commonwealth)

Key Points:

- Contains the Australian Privacy Principles – minimum standards to be met
- CSO records are generally bound by this Act. Right of access and correction of information applies regardless of when information was collected
- When collecting personal information from clients (e.g. application), inform them that information you are collecting is protected by the APP's and that they can have access to their personal information at any time (with sufficient notice). CSO's are required to have a Privacy Statement and Privacy Policy and this must be made available to anyone who requests it
- Upon client request, correct information to ensure it is accurate, up to date, complete, relevant and not misleading
- Generally, personal information cannot be passed on to others without the client's consent
- Information is to be locked away securely and protected from unauthorised access
- Withhold client information if it is believed on reasonable grounds that granting access would pose a serious and imminent threat to the life or health of the individual or any other individual. Provide the client with a written explanation of why the information is being withheld and their right to appeal to the Australian Information Commissioner
- If withholding personal information the organisation must, if reasonable, consider whether the use of agreed intermediaries would allow sufficient access to meet the needs of both parties.
- Generally, third party sensitive information should not be released without the consent of the third party.

Health Records Act 2001 (Vic)

Key Points:

- Health information means information or an opinion about: an individual's physical, mental, or psychological health, including any disability; and treatment or a health service an individual has received or will be receiving. Provide health information to the client as soon as possible.
- Most CSO client records are bound by this Act because the records likely contain health information
- The Act contains the Health Privacy Principles (HPP's) – minimum standards to be met. Note: if you are meeting the requirements of the HPP's then you are also generally meeting the APP's.
- The individual can make a request to you for access **orally** or in **writing**.
- The Act does not apply to information collected, used, disclosed, or held by an organisation prior to 1 July 2002. However, clients are entitled to a summary of their health information if that health information was collected prior to July 2002.
- Information must always be securely stored and protected from unauthorised access
- Clients must not be given access to information if it is believed on reasonable grounds that granting access would pose a serious threat to the life or health of the individual or any other individual.
- Access must not be given to health information that was originally given in confidence by a private individual, not an organisation. Access refusals must be done formally (refer to Act).
- Information cannot be passed on to third parties without the client's consent.

Adoption Act 1984 (Vic)

Key Points:

- Amendments to this Act were made by the Victorian Parliament in May 2013 and these amendments include natural parents having access to identifying information about their adult adopted children; and an optional 'contact statement', that allows an adopted person to nominate what type of contact they wish to have with their natural parents, including a desire for no contact
- Only Department of Human Services (DHS) approved and registered adoption agencies may provide any information relating to adoptions. Access to client information held by unregistered CSO's will need to be arranged through a registered agency e.g Connections UnitingCare.
- Clients will be required to attend a mandatory interview with the registered agency in order for the information to be released.
- Client consent is required prior to giving client records to another agency.

Evidence (Document Unavailability) Act 2006 (Vic)

Key Points:

- This Act allows a court to make any orders it considers necessary to correct unfairness to a party as a result of the unavailability of a document. A document is considered to be unavailable when it is no longer in the possession of a party to the proceedings, or it has been concealed, rendered illegible, undecipherable or incapable of identification.

Crimes Act 1958, Part 1, Division 5 (Vic)

Key Points:

- A document or any other thing that is, or is reasonably likely to be, required as evidence in a legal proceeding must not be destroyed. This applies to a legal proceeding that is in progress or is to be, or may be, commenced in the future.
- A document is considered to be destroyed if it has been physically destroyed, concealed, rendered illegible, undecipherable or incapable of identification.
- The penalties for destroying information are severe and include up to 5 years in jail. Both individuals and corporations may be prosecuted.

2.0 A Broad Approach to Administering Access – in Lieu of 'Forgotten Australians' Senate Report

CSOs are encouraged to implement the recommendations of the Senate Community Services Reference Committee Report - *"Forgotten Australians: A report on Australians who as children experienced institutional or out-of-home care"* (the Report). In the spirit of the Report, CSOs should where possible, apply a more liberal interpretation and application of the relevant Privacy Acts thereby assisting our care leavers to: (a) reconnect with their families and communities; and (b) develop a greater sense of identity and belonging.

3.0 Open Access Records (Historical Records)

All client records created in excess of 99 years ago will be deemed "historical" and are "open" for the public to access.

4.0 Closed Access Records

By convention, designated archival records regarding adults are withheld from public access for seventy-five (75) years and those concerning children (such as care leaver records) are closed for ninety-nine (99) years from the year in which the records were created.

This prevents the violation of personal privacy. Should someone wish to view the records of another, it is mandatory to obtain the written consent of that person (see Appendix 2- Sample 'Letter of Authority').
Normally, records in relation to a deceased person may only be viewed by the next of kin, or close blood relatives. Proof of death such as a death certificate should be provided if access is sought by the next of kin or blood relatives. In the absence of a death certificate, the CSO needs to be satisfied through other means e.g. verification by other people, funeral notice in paper etc. that the person to whom the records relate, is deceased.

5.0 Complaint Resolution and the Privacy Commissioners

Members of the public concerned about record storage and access matters as carried out by the CSO, may contact the Office of the Health Services Commissioner (for health records) and/or the Office of the Australian Information Commissioner (all records) for further clarification or action. The availability of the services of the Privacy Commissioners is to be made known to a person making a request if they are not satisfied with a CSO's access provisions and processes. A CSO's Privacy Statement and Privacy Policy should also include information about complaint resolution and how to contact the Privacy Commissioners.

6.0 Definitions

As per the Privacy Act 1988 and instruction from the Office of the Australian Information Commissioner, the following definitions apply to personal and sensitive information. A definition of records is obtained from the Australian Standard *AS ISO 15489-1:2001*.

Personal information - *personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*

a. *whether the information or opinion is true or not; and*
b. *whether the information or opinion is recorded in a material form or not.'*

Sensitive information **-** *this is information or an opinion about an individual's:*

- *racial or ethnic origin;*
- *political opinions;*
- *membership of a political association;*
- *religious beliefs or affiliations;*
- *philosophical beliefs;*
- *membership of a professional or trade association;*
- *membership of a trade union;*
- *sexual preferences or practices; or*
- *criminal record;*

sensitive information also includes health information and genetic information about an individual that is not otherwise health information.

Reasonable and reasonably - *reasonable and reasonably are not defined in the Privacy Act 1988*

The High Court of Australia has considered that what is reasonable is a judgement of fact and deciding what is reasonable will depend on each particular case and may be influenced by current standards. A reasonableness test implies the application of reasoned and objective judgement taking into account all known considerations and circumstances.

Records - *records are defined by the records management standard AS ISO 15489-1:2001 as: "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business". A record may consist of such formats as paper files, maps and plans, photographs, films, cards, books, registers and digital files.*

A record is considered to be a CSO "agency record" when the record is either produced or received by any CSO staff member in the course of their duties whilst employed by the CSO. Hence, a letter received by the CSO from a government department (as an example) becomes a document and record owned by the CSO. The "Best Practice" notes in this document deal specifically with administering access to information owned and in the possession of the CSO. In such cases the CSO becomes legally responsible for the administration of records access.

7.0 Guidelines for the Application and Issue of Client Records

Guidelines for the Application and Issue of Client Records	*Comment*
A person requesting access to client records may be any age.	*The Privacy Acts are not age specific.*
A request for a client record must relate to a client who previously received out-of-home care services from the CSO. The CSO, upon the client's (if care leaver) request, will endeavour to obtain the client's records from other CSOs and government agencies on the client's behalf.	
The application for client records will preferably be made in writing on the designated application form as provided by the CSO. Preferably, this form shall be completed as required noting that personal particulars will assist in locating the client's information. The person requesting the file will preferably provide their own personal particulars such as name, address and a contact number as well as sufficient information to enable the CSO to locate a person in previous care e.g. care leaver's name, date of birth etc. If gathering client information over the telephone, either before, or at the point of collecting the information, let the client know why the information is being collected and who will have access to it. Explain to the client any consequences of the client not providing personal information, such as the possibility of service limitations. Provide the client with a copy of the CSO's Privacy Statement and the CSO's contact details. Note: the Health Records Act also provides for applications for health information to be made verbally.	*Those clients limited in reading and writing skill may provide details over the telephone. CSO staff will obtain the information orally then send the prepared application to the enquirer for their signature.* *Alternatively, the CSO staff member need only satisfy themselves that they are providing the right records to the right person and a confirmation from a third person e.g. health professional, Minister etc will suffice. This process is to be documented.* *See Appendix 1 – Sample Application Form*
The person requesting the client record will be asked to provide a copy of photo ID such as a driver's licence and this will need to be submitted with the application. If photo ID is unavailable e.g. the client does not have a licence, other forms of identification shall suffice such as a medicare card, veterans affairs card, rates notice etc.	*The CSO staff member need only satisfy themselves that they are providing the right records to the right person. Keep the application process as simple as possible.*
The person (if care leaver) requesting a client record will generally have access to information about themselves and information about their family provided that the family information is not sensitive to the point of being of detriment (e.g. harm, damage, loss) to any family member.	*Provide as much family information as possible without unreasonably infringing on the privacy of living persons*

The person requesting a client record that is not their own will be required to obtain the written permission of the person whose client record it is. Similarly a person requesting their own records may use the same authority to nominate an agent to act on their behalf.	*See Appendix 2 – Sample 'Letter of Authority'.*
The application processing period is 30 days or less.	*Allowing up to 30 days will ensure a thorough search for records including contextual records*
Persons requesting client records that contain any information relating to adoption will be advised that due to legislative requirements, the records may only be released by registered adoption agencies. Arrangements are to be made for the records to be released through the Department of Human Services (DHS) or a DHS registered adoption agency such as Connections UnitingCare. Explain the process to the client and obtain client consent to send the records to the registered adoption agency. Special note: it will be necessary for the CSO to contact the registered agency for further advice (without disclosing personal particulars of the client) if it is likely that the client has no knowledge of their adoption. This should be done prior to contacting the client.	*Offer to facilitate this process for the client. Offer to attend the registered adoption agency with the client if they have no other support person.*
Client records will be issued in a culturally sensitive way.	*Appropriate advice and if necessary assistance shall be obtained by relevant cultural bodies (eg Link-Up, Connecting Home, Child Migrant Trust) prior to releasing culturally sensitive information.*
After applying the relevant privacy principles, a copy of the client information shall be provided to the client: (a) in a format preferable to the client, if possible; and (b) in its entirety such as the client file, the Admission Register entry, Ladies Committee Minute record entries, photographs etc. A search of family and sibling files will also be made to locate any further information relating to the client information being applied for.	*Information shall be provided in its entirety. If records are potentially available but are not sufficiently described to enable them to be accessed, inform the client of such and the CSO's plans for improving accessibility to the information.* *Provide the client with a list of the CSO's record holdings regarding care leavers. Place the same information in a public space e.g. Find and Connect website or the CSO's website.*

An electronic '**register of client access'** (spreadsheet) to information shall be maintained. Information captured shall include: name, address and contact details of applicant for information; name(s) of person who was in care; date of application; date information was sent to the applicant; and a file note of contact with the applicant and/or comments.

If you are documenting further client information over the telephone, either before, or at the point of collecting the information, let the client know why the information is being collected and who will have access to it.

Additionally, an electronic '**further contact register'** (spreadsheet) shall be maintained and this will note whether the client wants further contact or notifications from the CSO or others e.g. other care leavers, people that maintained contact with the care leaver as a child, reunion activities etc.

This information – apart from the 'further contact register', as well as copies of client records issued will be destroyed after 7 years.

A copy of records shall be provided free of charge to the client.

The physical release of records shall be conducted by the CSO in a manner that satisfies the client. Options for the client may include the client meeting with the CSO in a supportive environment either at the CSO premises or elsewhere, the CSO delivering the records to aged and infirm persons, or the CSO posting the records by registered post. The CSO shall take precautions as to their duty of care when providing the client with sensitive information.

The manner of release of the records to the client will be a discussion with the client. The CSO will offer supported release of information at all times, including follow-up where appropriate and with the client's consent.

Clients who are care leavers or their family members shall receive advice both verbally and in writing, at the time of application, about support, assistance and information services available to care leavers and their families

In the spirit of the 'Forgotten Australians' Senate Report care leavers and their families will be given maximum assistance and information to allow them to reconnect with their families and communities and to establish matters of identity and fact.

CSOs are encouraged to provide an information kit for care leaver clients and their families. The kit, both paper and electronic versions, would be inclusive of: all application forms; a privacy statement or policy (that includes why we require application details, who will access the information, how long we retain information for, access to and correction of information etc.); agency information; internal and external support services; and resources for care leavers, including the provision of brochures.

8.0 Best Practice Notes for Administering Records Access to Care Leavers

What do I do with information concerning third parties? What can I leave in?

APP = Australian Privacy Principles
HPP = Health Privacy Principles

Information on File Concerning:	*Comment (Delete/Leave etc)*	*Applicable Privacy Code*
Self (Care Leaver or Their Representative)		
All particulars relating to the client (including legal, police and health reports). Not including adoption information	**Leave**, unless: (a) you reasonably believe that giving access would endanger the life, health or safety of any individual or public health or safety; (b) giving access would be unlawful; and (c) providing access would have an *unreasonable* impact on the privacy of other people.	APP 12.1; 12.3(a); 12.3(b); 12.3(f)
	If refusing to provide information, the CSO must provide the client with a written notice with the reason for refusal except to the extent that, having regards for the grounds for refusal, it would be unreasonable to do so.	APP 12.9
	Health information collected pre 1 July 2002 may be given in summary form concerning facts not opinions however, if possible, provide information in its entirety. If denying health information you must provide the client with written reasons for doing so and the option of having an independent review of the decision (refer to Act). Provide health information as soon as possible to the client.	HPP 6.1
	Note: confidential information would normally be released. The term 'confidential' or 'not to be disclosed to a third party' has no legal effect unless that document was provided by a **private person**. The CSO or a health service provider or any other organisation cannot claim confidentiality. Confidential information may only be denied if providing that information seriously endangers the life of the individual or any other individual or the information is being withheld for a lawful matter.	Section 26 and 27 HRA
	Provide the client with originals records such as photos of themselves, letters written to/by the client and school reports. Retain copies on the client's file.	APP 12.3
	Correct information if: (a) a client requests you to do so in the event that the information is inaccurate, incomplete, misleading or not up to date; and (b) it is reasonable to correct that information. If information is not being	APP 13.1 – 13.4

	corrected, inform the client in writing the reason for refusal and processes available for the client to complain about the refusal. Additionally, offer the client the option of associating (adding) a statement with the information as an addendum.	
All particulars relating to the client and adoption information	**Refer** the entire file to a Registered Adoption Agency e.g. Connections UnitingCare or the Family Information Networks Discovery (FIND) unit at DHS. Facilitate the process of connecting the client with the relevant agency and offer the services of being a support person if the client does not already have one.	Adoption Act 1984
All particulars relating to a client with an Australian Indigenous background	**Seek** appropriate advice and assistance from the organisation Connecting Home (Vic) regarding the sensitive release of information and meeting Connecting Home protocols. Administer access as per this guide if appropriate and consistent with Connecting Home protocols.	
Parents and Grandparents		
Names and addresses	**Leave**, parents and grandparents would reasonably expect the CSO to disclose this information. In general, a person would know who their grandparents are. Additionally, this information is necessary for family reunification and to establish or confirm identity and belonging.	APP 6.2(a)
Information concerning the parents/grandparents name – that is (a) not on a birth certificate or in any other record other than the client file; or (b) inconsistent with the care leaver's knowledge	**Leave**, it is possibly the only information confirming the parents or grandparents name. Follow protocols similar to the release of adoption information e.g. asking the client to attend the CSO, or negotiate another supportive environment, so that the content of the records may be discussed and support rendered to the client.	APP 6.2(a)
Letters written by the CSO, the Department (e.g. Child Welfare Department) or other organisations to parents or grandparents or vice versa	**Leave**, unless the information is sensitive and the parent or grandparent is reasonably likely to suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued.	APP 6.2(a)
Personal particulars relating to parents or grandparents e.g. education, domestic circumstances, activities that they are engaged in etc.	**Leave**, unless the information is sensitive and the parent or grandparent is reasonably likely to suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued.	APP 6.2(a)

Sensitive particulars relating to a parent or grandparent e.g. personal habits, actions and activities of a sensitive nature, sensitive disclosures made by the individual etc.	**Delete** if it is reasonably likely that: a parent or grandparent will suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued; the parent or grandparent would not want the CSO to disclose the information.	APP 6.2(a) HPP 2.2
Information concerning visits to the child or the child visiting the parent or grandparent	**Leave**, parents and grandparents would reasonably expect the CSO to disclose this information. The purpose of the visit was to maintain contact with the child. Additionally, this information is necessary for family reunification.	APP 6.2(a)
All information concerning a deceased parent or grandparent	**Leave**, privacy is not extended to deceased persons only natural persons. Additionally, the client is a close blood relative.	
Siblings		
Names of siblings	**Leave**, it is likely that siblings would reasonably expect the CSO to disclose this information. In general, a person would know the names of all their siblings. Additionally, this information is necessary for family reunification.	APP 6.2(a)
Address and contact details	**Leave**, it is likely that siblings would reasonably expect the CSO to disclose this information. In general, a person would know the address and contact details of their siblings. Additionally, this information is necessary for family reunification. **Delete**, if you have had previous contact with the sibling and the sibling has asked that this information remains private. If appropriate check again to establish if the sibling still wants their details kept private.	APP 6.2(a)
Personal particulars relating to siblings e.g. education, domestic circumstances, activities that they are engaged in etc.	**Leave**, it is likely that siblings would reasonably expect the CSO to disclose this information. In general, a person would know personal particulars relating to siblings.	APP 6.2(a)
Sensitive particulars relating to siblings e.g. personal habits, actions and activities of a sensitive nature, sensitive disclosures made by the individual etc.	**Delete** if it is reasonably likely that: a sibling will suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued; the sibling would not want the CSO to disclose the information.	APP 6.2(a) HPP 2.2

References to siblings and client in the same context e.g. John and Betty (siblings) went to camp	**Leave**, unless the information is sensitive and the sibling is reasonably likely to suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued. .	APP 6.2(a)
Information concerning visits to the child or the child visiting the sibling	**Leave**, it is likely that siblings would reasonably expect the CSO to disclose this information. Additionally, this information is necessary for family reunification.	APP 6.2(a)
Information concerning a deceased sibling	**Leave**, privacy is not extended to deceased persons only natural persons. Additionally, the client is a close blood relative.	
Relatives		
Names of relatives	**Leave**, it is likely that relatives would reasonably expect the CSO to disclose this information. In general, a person would know the names of their relatives. Additionally, this information is necessary for family reunification.	APP 6.2(a)
Address and contact details	**Leave**, it is likely that relatives would reasonably expect the CSO to disclose this information. In general, a person would know the address and contact details of their relatives. Additionally, this information is necessary for family reunification.	APP 6.2(a)
Letters written to/from the CSO	**Leave**, unless the information is sensitive and the relative is reasonably likely to suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued.	APP 6.2(a)
Personal/sensitive particulars relating to relatives e.g. economic circumstances, health status, education, domestic circumstances etc.	**Delete**, if it is reasonably likely that: a relative will suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued; the relative would not want the CSO to disclose the information.	APP 6.2(a) HPP 2.2
Information concerning visits to the child or the child visiting the relative	**Leave**, most people visiting the child would have done so for the primary purpose of maintaining contact with the child. Additionally, this information is necessary for family reunification.	APP 6.2(a)
External Carers e.g. Holiday Hosts		
Names of carers	**Leave**, it is likely that carers would reasonably expect the CSO to disclose this information. In general, a person would know the name of their carer.	APP 6.2(a)

Address and contact details of carers	**Delete**, but offer to facilitate a process of contacting the carer on the client's behalf should the client seek contact with the carer.	APP 6.2(a)
Letters written by the CSO, the Department (e.g. Child Welfare Department) or other organisations to carers or vice versa	**Leave**, unless it is reasonably likely that any of the following apply: (a) the carer will suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued; (b) the carer would not want the CSO to disclose the information; or (c) the information does not directly relate to the client. **Delete**, address and contact details of carers.	APP 6.2(a)
Internal Carers e.g. CSO Staff		
Names of carers and staff e.g. Cottage Mother	**Leave**, it is likely that carers and staff would reasonably expect the CSO to disclose this information. In general, a person would know their carers (or staff) names.	APP 6.2(a)
Address and contact details of carers and staff	**Delete**, but offer to facilitate a process of contacting the carer or staff on the client's behalf should the client seek contact with the carer or staff.	APP 6.2(a)
Letters written by the CSO, the Department (e.g. Child Welfare Department) or other organisations to carers/staff or vice versa	**Leave**, unless it is reasonably likely that any of the following apply: (a) the carer will suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued; (b) the carer would not want the CSO to disclose the information; or (c) the information does not directly relate to the client. **Delete**, address and contact details of carers/staff.	APP 6.2(a)
Other, Non Related Children in the Home		
Names of other children in the Home	**Leave, the clients first name** – it is likely that the care leavers (other children) would reasonably expect the CSO to disclose this information. In general, a person would know the names of other children they grew up with. Additionally, names, places and dates assist a client to remember facts about their time in care. Note: delete family names of other children - some care leavers have expressed not having their family name disclosed due to the potential of information later appearing in electronic social media. Consider that not all care leavers have disclosed that they were in care.	APP 6.2(a)

Contact details of other children in the Home.	**Delete**, but offer to facilitate a process of contacting the other care leaver on the client's behalf should the client seek contact with the other care leaver.	APP 6.2(a)
References to other children and the client in the same context e.g. David (other child) and Mark (client) played on the swings	**Leave**, unless the information is sensitive and the other care leaver is reasonably likely to: suffer a detriment (e.g. hurt, damage, loss) as a result of the information being issued; not want the CSO to disclose the information. Note: delete family names of other children - some care leavers have expressed not having their family name disclosed due to the potential of information later appearing in electronic social media. Consider that not all care leavers have disclosed that they were in care.	APP 6.2(a)
Any other personal and sensitive particulars of other children with the exception of photos	**Delete**, this is private third party information and the subject matter relating to being in care is generally very sensitive in nature. It is reasonably likely that the individual would not want their personal information released.	APP 6.2(a)
Photo(s) that include other children, staff, other people	**Leave**, if one of the children in the photo(s) is the person making the request. If the photo is post 1 January 1955, attach a label to the back of the photo indicating that the photo is copyright of the CSO or photographer and subject to the Copyright Act 1968. Photos of people are not to be provided if the client is not in the photo unless those photos have been previously published or the photos are of group events e.g. special functions, celebrations etc.	APP 6.2(a)
Government Departments and Other Organisations (including Health Service Providers)		
Name, address and contact details of service providers and organisations	**Leave**, privacy legislation does not protect businesses and their staff operating in a business capacity, only private persons.	
Correspondence and reports including school reports, health reports, police reports	**Leave**, unless: (a) you reasonably believe that giving access would endanger the life, health or safety of any individual or public health or safety; (b) giving access would be unlawful; and (c) providing access would have an *unreasonable* impact on the privacy of other people. **Delete** all names, contact details and other personal particulars of all other private persons (third parties) if giving access would have an unreasonable impact on the privacy of that other person. Private person does not include employees of organisations and service providers.	APP 12.1; 12.3(a); 12.3(b); 12.3(f)

	If the client wants contact details of other private persons (not including employees of other organisations) assist the client by obtaining the information from a public source or offer to be an intermediary by contacting the other private person and providing the care leaver's contact details (if agreed by the care leaver).	

APPENDIX 1

SAMPLE

RECORDS REQUEST APPLICATION

Lentara UnitingCare uses this form to locate the records you have requested and to ensure that they are appropriately accessed. The use, disclosure and security of information are some of the privacy matters addressed in our *Privacy Statement* to you (attached).

Please complete the form with as much known information as possible. The details you provide on this form are protected by privacy legislation.

Details of the Person Making the Inquiry

Date:	
Name:	
Address:	
Telephone:	(H) (W or Mob)
Best time to phone	
Relationship to Person named below	

Information Regarding Person Placed in Care

Family Name(s):	
Given Names:	
Date of Birth:	
Mother's Name:	
Father's Name:	
Approx. Year Admitted to Care	
Approx. Year Left Care	
Siblings:	
Name of Homes or Services if Known	

Supporting Documentation

Please tick boxes as appropriate and attach copies of the documents concerned	Either of the following two primary documents is required: ☐ A copy of your photo Driver's License ☐ A copy of your Passport Plus, where relevant any of the following documents: ☐ Evidence of a name change (e.g. marriage certificate) ☐ A copy of death certificates (if you wish to view information about your parents or siblings and they are deceased)
Are you searching for health information?	☐ Yes, general information OR ☐ Yes, urgent and specific information

Affirmation and Consent

I affirm that the information I have provided is true and correct and I authorise Lentara UnitingCare to conduct a record search and provide me with the information requested.

Signature……Date……...

Important note: for information about third parties such as your parents or siblings, we require their permission to release any information about them (a Letter of Authority Form is attached). If you are unable to supply us with written permission from them, we are obliged by Privacy legislation to delete some specific information about them. If your parents or siblings are deceased, we require confirmation of this, such as a copy of a Death Certificate, alternatively please contact our Care Leaver Support Worker for further information.

Return to:
In Confidence
Care Leaver Support Worker
Lentara UnitingCare,
PO Box 3217
BROADMEADOWS VIC 3047

Thank-you for completing this application.
Please allow up to 30 days for the processing of your application

APPENDIX 2

SAMPLE

LETTER OF AUTHORITY

This form is only to be completed if you are asking another person to act on your behalf or you are giving consent for Lentara UnitingCare to release third party information about you to the person nominated below.

To: Care Leaver Support Worker
Lentara UnitingCare
PO Box 3217
BROADMEADOWS VIC 3047

I ……..
(PRINT FULL NAME OF PERSON GIVING THE AUTHORITY/CONSENT)

Of ……...
(PRINT FULL ADDRESS OF ABOVE PERSON)

duly authorize the following named person to either (a) act as my agent or representative or (b) receive information about me (cross out and initial that which does not apply):

……
(PRINT FULL NAME OF PERSON)

Limits to this authorization: (cross out and initial that which does not apply)

- To contact Lentara UnitingCare on my behalf to request an archive search for information.
- To receive any information from archived files on my behalf.
- For Lentara UnitingCare to release third party information about me.
- Other, including **NOT** wanting the release of specific information (please specify information not to be released)

……..……...

……..……

Duration of this authorisation:

- The completion of the archive search inquiry.
- As otherwise advised or instructed (please specify)……..…

Signed ……..……..…..Dated ……..…

APPENDIX 3

THE AUSTRALIAN PRIVACY PRINCIPLES (APP'S)

Part 1 — Consideration of personal information privacy

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.

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.

Part 2 — Collection of personal information

Australian Privacy Principle 3 — collection of solicited personal information

Personal information other than sensitive information

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

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

Sensitive information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Means of collection

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

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

(a) if the entity is an agency:

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

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

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

Solicited personal information

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

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.

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

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

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

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

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

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

(b) if:

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

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

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

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

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

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

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

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

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

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

(j) if the APP entity is likely to disclose the personal information to overseas recipients — the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3 — Dealing with personal information

Australian Privacy Principle 6 — use or disclosure of personal information

Use or disclosure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.4 If:

(a) the APP entity is an organisation; and

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

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

Written note of use or disclosure

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

Related bodies corporate

6.6 If:

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

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

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

Exceptions

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

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

(b) government related identifiers.

Australian Privacy Principle 7 — direct marketing

Direct marketing

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

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

Exceptions — personal information other than sensitive information

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

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

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

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

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

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

(a) the organisation collected the information from:

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

(ii) someone other than the individual; and

(b) either:

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

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

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

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

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

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

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

Exception — sensitive information

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

Exception — contracted service providers

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

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

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

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

Individual may request not to receive direct marketing communications etc.

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

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

or

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

the individual may:

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

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

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

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

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

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

Interaction with other legislation

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

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

(b) the *Spam Act 2003*;

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

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.

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).

Part 4 — Integrity of personal information

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.

Australian Privacy Principle 11 — security of personal information

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

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

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

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

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

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

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

Part 5 — Access to, and correction of, personal information

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; or

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

Dealing with requests for access

12.4 The APP entity must:

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

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

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

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

Other means of access

12.5 If the APP entity refuses:

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

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

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

Access charges

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

12.8 If:

(a) the APP entity is an organisation; and

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

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

Refusal to give access

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

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

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

(c) any other matter prescribed by the regulations.

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

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).