Managing Personal Information under the Australian Privacy Principles Procedures

As a centre for Social Enterprise, FSG Australia is committed to delivering on the values of Freedom, Social Justice and Growth.

www.fsg.org.au

V14 – 24/5/16 **Document is considered uncontrolled once printed**

TABLE OF CONTENTS

SECTION A – INTRODUCTION

Glossary

Refer to FSG Australia glossary

Scope

This document applies to all FSG Australia (FSGA) workers unless exceptions are listed in this scope.

A person is a worker if the person carries out work in any capacity for FSGA, including work as:

(a) an employee; or

(b) a contractor or subcontractor; or

(c) an employee of a contractor or subcontractor; or

(d) an employee of a labour hire company who has been assigned to work at FSGA or

(e) an outworker; or

(f) an apprentice or trainee; or

(g) a student gaining work experience; or

(h) a volunteer.

Customers may be adults, young persons or children.

These procedures only apply to personal information managed under the *Privacy Act 1988 (Cwlth)* which legislates the Australian Privacy Principles (APPs).

i) Additional procedures apply to information and file management related to children and young people placed with FSGA by the Department of Communities, Child Safety and Disability Services - Child Safety Services (refer to the Kaia Program Practice Manual - Foster Care, KAIA Program Practice Manual - Residential Care Services and KAIA File Management Procedures).

ii) Additional procedures apply to the Commonwealth Respite and Carelink Centre, and the service manager is responsible for implementing program-specific procedures as detailed in the Australian Government Department of Health & Ageing Operational Manual for Commonwealth Respite and Carelink Centres and the funding agreement.

iii) Information about deceased persons does not fall within the definition of personal information in the Privacy Act. So, the Privacy Act does not apply to any information about deceased people. However, the Privacy Act could apply if the information also includes or divulges personal information about a living person.

iv) The handling of employee personal information is outside of the scope of this policy if it is directly related to:

- current or former employment relationship
- an employee record relating to an employee.

This means that FSGA does not need to comply with the APPs when it handles current and past employee records. This also means that FSGA does not have to grant employees access to their employee records. This exemption does not apply to volunteer or contractor records. However, prospective and former employees' personal information is covered by this policy.

v) When FSGA is operating as an agency for the Queensland Government the information specifically related to the program may not be covered by the APPs, in this instance refer to the program manual e.g. Housing Manual for procedures related to tenant information.

vi) Refer also to the RTO Manual for procedures related to student information.

vii) Refer also to the Assets Management Policy for additional procedures related to contractor information.

viii) Refer also to the Governance and Management Manual for procedures related to Board Members and approved Associates confidentiality and privacy requirements.

ix) Other legislation related to funding agreements may need to be taken into account when reading these procedures.

X) For relevant headspace Capalaba procedures refer to: headspace Capalaba Privacy Policy..

FSG Australia overarching policy is available at FSG Australia Overarching Policy.

There is a requirement for line managers to include these procedures in work area orientation

Human Services Quality Standards

Standard 1: Governance and management

7. The organisation has effective information management systems that maintain appropriate controls of privacy and confidentiality for stakeholders.

Home Care Standards

Standard 1: Effective management

1.2 The service provider has systems in place to identify and ensure compliance with funded program guidelines, relevant legislation, regulatory requirements and professional standards.

Standard 3: Service user rights and responsibilities

3.2 Each service user's right to privacy, dignity and confidentiality is respected including in the collection, use and disclosure of personal information.

National Standards for Disability Services

Standard 6: Service management

1:1 The service, its staff and its volunteers treat individuals with dignity and respect.

1:9 The service keeps personal information confidential and private.

NSW Disability Service Standards

Standard 1 - Rights

4. Each person will receive a service that reflects their right to privacy and have their personal records and details about their lives dealt with in an ethical and confidential manner in line with relevant legislation

Policy (summary)

APP1

- FSGA has a clearly expressed and up-to-date privacy policy
- FSGA takes reasonable steps to implement processes that will ensure that FSGA complies with the APPs

APP 2

- FSGA allows individuals to interact with the organisations by not identifying themselves
- FSGA permits the individual to use a pseudonym except when it is impracticable for FSGA to deal with an unidentified individual

APP 3

- Collection of personal information is ‘reasonably necessary’ for one or more of FSGA’s functions or activities

APP 4

- When receiving unsolicited information FSGA establishes if the information could have been collected under APP 3 and destroys or de-identifies the information if it could not have been collected under APP 3

APP 5

FSGA informs an individual of when the organisation collects their personal information. These matters include:

- who FSGA is and how to contact us
- the purpose(s) of the collection
- any collections from third parties
- consequences of non-collection
- complaint handling process
- potential overseas disclosure.

APP 6

Care is taken to ensure that personal information is only used/disclosed if it is related to the purpose for which it was collected and within the reasonable expectations of the person to whom the information relates. FSGA takes steps to ensure the quality of used/disclosed information. The legality of using/disclosing personal information for a secondary purpose is checked before release/use.

APP 7

Care is taken to ensure that FSGA complies with marketing-related use of information.

App 8

FSGA takes reasonable steps to ensure personal information it collects, uses or discloses is:

- accurate
- up to date
- complete.

FSGA ensures that personal information that it uses or discloses is also relevant for the purpose of the use or disclosure.

APP11

FSGA takes reasonable steps to protect personal information it holds from misuse, interference and loss and from unauthorised access, modification or disclosure

APP 12

FSGA responds to requests for access of personal information within a reasonable timeframe.

Access is provided in the requested manner (where reasonable and practicable).

Written reasons for the refusal is given and the complaint mechanism.

FSGA does not excessively charge for access to personal information and charges do not apply to the making of the request.

APP 13

- FSGA takes ‘reasonable steps’ to correct personal information to ensure that it is accurate, up to date, complete, relevant and not misleading, if either:
  - FSGA is satisfied it needs to be corrected, or
  - individual requests correction.
- FSGA produces a statement if declining to correct and the individual requests statement
- FSGA responds in a reasonable period
- FSGA provides written reasons for refusal and the complaint mechanism

SECTION B - PROCEDURE

1.0 Providing information to a person from whom personal information is to be collected

1.1 All workers

Prior to collecting personal information you must inform the person from whom you are collecting the information of FSGA's privacy policy in a manner which is in a suitable format. If requested, you must provide access to the information in this document in the requested format unless the request is unreasonable.

Any worker who is responsible for gathering personal information to hold/use must ensure that the person from whom they are gathering the information is provided with sufficient information to make an informed decision to consent to them disclosing that information.

Information provided to the person is to include:

- the kinds of personal information FSGA will collect and hold e.g. contact details, employment history, educational qualifications, complaint details
- sensitive information collected or held by FSGA listed separately listed e.g. mental health, disability, racial or ethnic origin, criminal convictions, religious affiliation, political affiliation, and tax file numbers
- FSGA's usual approach to collecting personal information e.g. whether personal information is collected directly from people or from list purchases, competitions, or referrals from individuals or other entities
- FSGA's usual approach to holding personal information, including storing and securing information
- purposes for which personal information is usually collected, held, used and disclosed. This description will usually indicate the range of people or entities that may access that personal information
- the procedure a person can follow to gain access to or seek correction of personal information
- that people have a right to request access to their personal information and to request its correction and

- the position title, telephone number and email address of a contact person for requests to access and correct personal information
- how a person can complain about a breach of privacy (including the procedure and contact details for complaining directly to FSGA and the procedure for complaining to an external complaint body
- whether personal information is likely to be disclosed to overseas recipients and the countries in which such recipients are likely to be located; if it is practicable to specify those countries in the policy
- who, other than the person to whom the information pertains, can access personal information, and the conditions for access
- the period for which personal information records are kept
- FSGA's process or schedule for updating its privacy procedures and how changes will be publicised
- the situations in which a person can deal with FSGA by not identifying themselves or using a pseudonym. You are responsible for ensuring that all information provided to persons prior to FSGA providing a service clearly states that they have the opportunity to deal anonymously or by pseudonym. This may be stated verbally, printed on a form or as a notation on an online data collection tool e.g. unless it is impractical for us to respond in relation to a particular request, you may choose not to identify yourself and to deal with us anonymously.

To meet this requirement the FSGA privacy statement and policy are available at www.fsg.org.au. People from whom FSGA collects personal information should be directed to this policy.

1.2 Coordinators/Managers

You are responsible for developing other service/department-specific privacy information sheets where it is believed that the website format and/or location are not suitable for people from whom you collect personal information .

For Disability, Aged Care & Mental Health Services there is a pictorial Privacy of personal information fact sheet - pictorial to give to those persons for whom pictures will facilitate understanding and Fact Sheet 8 Privacy Fact Sheet which is easy to read.

You are responsible for developing scripts for workers who collect personal information over the phone.

1.3 Controlled Document Manager

You are responsible for:

- placing the privacy logo on all forms recording personal information
- placing a privacy notification on all forms which the individual about whom the information pertains will complete
- ensuring forms which collect personal information from a third party record that the third party has informed the individual about how they are using their personal information.

2.0 Responsibility for promoting worker awareness of the APPs

2.1 Human Resources

When conducting the recruitment process of an employee you are responsible for ensuring that prior to employment the new recruit signs a role-specific contract agreeing to maintain the privacy of personal information and that this document is placed on the person's personnel file.

2.2 Volunteering FSGA Senior Coordinator

You are responsible for ensuring that FSGA volunteers sign a Volunteer, students and friends of FSGA confidentiality & privacy agreement form and that the signed form is placed on file (refer also to the Volunteering FSGA Operations Manual).

2.3 Line Manager of contractors

You are responsible for ensuring that contractors sign the Confidentiality & privacy agreement form, if they have not already signed other documentation which pledges their agreement to comply with the legal requirement to protect personal information. You are responsible for placing the signed form on the program/department file.

This information may also be gathered on the Approved Tradesperson, Contractor or Supplier Agreement used by Realty for approved tradespersons or contractors.

2.4 Line Managers

You are responsible for ensuring that employees are informed in work area orientation about service-specific confidentiality requirements. A record is kept of this in accordance with the Work area orientation manual - procedures for line managers.

2.5 Privacy Advisor

You are responsible for advising workers on the implementation of the APPs.

2.6 All workers

You are responsible for complying with the APPs and reporting any breaches as an incident (refer to Managing Incidents Procedures).

Prior to collecting personal information you must inform the person from whom you are collecting FSGA's privacy procedures (refer to 1.0 Providing information to a person from whom personal information is to be collected).

2.7 Marketing

You are responsible for ensuring that current information about FSGAs procedures related to personal information is available at all times on the FSGA website.

2.8 Controlled Document Manager

You are responsible for ensuring information given to persons before the collection of personal information meets legislative and best practice requirements (refer to 1.0 Providing information to a person from whom personal information is to be collected).

2.9 Staffing Solutions Service Manager

You are responsible for ensuring that contracts are in place with organisations which deploy contract workers to FSGA. These contracts are to specify that contract workers are to adhere to FSGA's privacy policy.

2.10 Learning & Development Manager

You are responsible for ensuring that students (other than employees) completing any tasks which will give them access to relevant personal information e.g. students completing vocational placement, sign a Volunteer, students and friends of FSGA confidentiality & privacy agreement form and that the signed form is placed on file.

3.0 Responsibility for formally managing risk to privacy of personal information

3.1 Governance

For governance risk management roles and responsibilities refer to the Governance and Management Manual.

3.2 Internal Auditor

In consultation with the IT Manager you are responsible for ensuring that risks associated with privacy are assessed as part of the quality audit. This is to include each stage of the information lifecycle, including collection, use, disclosure, storage, destruction and de-identification.

You are responsible for conducting a periodic review of the adequacy and currency of FSGA's privacy procedures and of the practices, procedures and systems implemented under APP.

4.0 Collecting personal information

Also refer to 5.0 Photographs, film

4.1 All workers collecting personal information

You should only collect the personal information necessary to provide a service (this is best controlled by the use of an FSGA-approved data collection tool).

You must provide notification before, or at the time you collect personal information (if this is not practicable, notification should be provided as soon as practicable after collection) of:

- FSGA's identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- the consequences if personal information is not collected
- FSGA's usual disclosures of personal information of the kind collected
- information about FSGA's privacy procedures (refer to 1.0 Providing information to a person from whom personal information is to be collected)

- You may only collect personal information that is reasonably necessary for, or directly related to, one or more of FSGA's functions or activities.
- You may only collect sensitive information if the person consents to the sensitive information being collected, unless an exception applies (refer to APP 3.3)
- You must collect personal information:

- only by lawful and fair means (refer to APP 3.5), and
- directly from the person, unless an exception applies (refer to APP 3.6 and 4.3 Collecting information from a third party).

4.2 Coordinators/Managers

You must take such steps (if any) as are reasonable in the circumstances to ensure the quality of personal information when it is collected (at this point it must ensure that the personal information is accurate, up to date and complete). Procedures required to check the quality are:

- all personal information is to be collected on FSGA-approved forms
- procedures are to be in place to check the accuracy and completeness of the information by reminding individuals regularly (at least annually) to update their personal information
- information provided by a third party is to be checked with the individual or decision maker
- updated or new personal information is promptly added to relevant existing records
- reviewing data collection tools regularly with the purpose of removing unnecessary data collection.

4.3 Collecting information from a third party

APP 3.6 provides that FSGA 'must collect personal information about an individual only from the individual', unless it is unreasonable or impracticable for the entity to collect personal information only from the individual

Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned will depend on the circumstances of the particular case. Considerations that may be relevant include:

- whether it is difficult to collect the information directly from that individual
- whether the individual would reasonably expect information about them to be collected directly from them or from another source
- the sensitivity of the information being collected
- whether direct collection would jeopardise a purpose of collection or the integrity of the information collected

- whether the cost of collecting directly from the individual would be excessive
- any privacy risk if the information is collected from another source.

When workers are responsible for receiving personal information from a third party they should consider if it is reasonable and practical to check that the third party, from whom personal information is collected, has implemented appropriate data quality practices, procedures and systems e.g. where there is a contract in place making enforceable contractual arrangements to ensure that the third party implements appropriate data quality measures in relation to the personal information FSGA collects from the third party.

Records of consent to the collection of information from a third party are kept on Consent to collect personal information from a third party.

5.0 Photographs, film

Reference: https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/businesses/what-do-i-need-to-think-about-if-i-want-to-put-photographs-or-video-of-people-on-the-web

Images of individuals in photographs or film are treated as personal information under the APPs where the person's identity is clear or can reasonably be worked out from that image. Consent is not required to collect photographs of identifiable individuals unless the picture records sensitive information about the individual. However, FSGA must take reasonable steps to tell the individual who FSGA is, what FSGA is taking their picture for, and how they can get access to it later.

As individuals may be sensitive to their pictures being published their consent must be sought. Where more than one person is represented in an image, consent must be obtained from everyone, even though the primary focus might be on a single person.

In consultation with Marketing, consent is recorded on the Marketing Consent and release form.

FSGA will require consent to use the picture for something other than what the individual(s) would reasonably expect.

The APPs protect the personal information of both adults and children alike. FSGA takes particular care in the handling the images and other personal information of children. Depending on the age and ability of the child to understand FSGA's explanation about what is going to happen with their picture and to make a truly informed choice, FSGA seeks consent from a parent or guardian first.

It is prohibited under s189 of the *Child Protection Act 1999* to publish information which identifies, or is likely to identify, a child or young person in the context of intervention by the

child safety system without the written approval of the Child Safety Service's Director-General.

6.0 Marketing

Any workers involved in marketing must be aware of and comply with APP 7. Among other requirements APP7 requires that FSGA must not use or disclose personal information for the purpose of direct marketing unless an exception applies.

Direct marketing involves communicating directly with an individual to promote goods and services.

Where FSGA is permitted to use or disclose personal information for the purpose of direct marketing, it must always:

- allow an individual to request not to receive direct marketing communications (also known as 'opting out'), and
- comply with that request.

FSGA must provide its source for an individual's personal information, if requested to do so by the individual.

7.0 Surveys and feedback

Wherever possible formal surveys and feedback should be answered anonymously and processed centrally.

8.0 Workers receiving unsolicited personal information

You must, as soon as practicable, destroy or de-identify, if it is lawful and reasonable to do so, unsolicited personal information received by you, that could not have been collected under APP 3 (for more information refer to APP 4.3).

If you receive information from a person other than the person to whom the information relates or another organisation you are required to notify the person:

- that personal information has been collected and from which organisation (or from which individual providing this is not breaching their privacy)
- the circumstances of the collection, such as the date, time, place and method of collection.
- the purposes for which FSGA collected the personal information. This should include the primary purpose of collection, that is, the specific activity for which particular personal information is collected. If FSGA may use or disclose personal information for another purpose (known as a 'secondary purpose'), this should also be noted.

9.0 Managing complaints about breaches of privacy

The APPs state that the complainant should take their complaint to FSGA before making a complaint to the Privacy Commissioner.

9.1 All workers

If you are approached in relation to a complaint about a privacy breach you are to inform the complainant that they are required to put their complaint in writing and send to the FSGA Customer Liaison Officer at:

PO Box 2597, Southport 4215

or

Email: complaints@fsg.org.au

9.2 CEO

If the complainant remains dissatisfied with the outcome after the procedures in Managing Complaints Procedures are followed, you are required to refer the complainant to the Office of the Australian Information Commissioner (15.0 Privacy Commissioner contact details).

In accordance with Process Improvement Procedures you are required to ensure that:

- systemic issues are improved; actions may include:
    - privacy training for all relevant employees/volunteers
    - amendment of forms and/or collection notices
    - improved security and storage measures
    - steps to improve data accuracy
- recording any changes are made
- reviewing privacy procedures after privacy complaints or breaches.

10.0 Managing electronic information for customers of disability, aged and mental health services personal information

Note: This section is not relevant to the Commonwealth Respite and Carelink Centre

This section applies to records located at: \\Fsgstore001\data\CLIENTS.

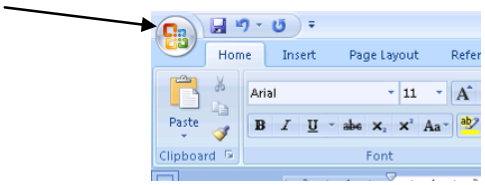
For procedures related to records on TRACCS refer to TRACCS recipient management training material.

When saving personal information, extra care is required to ensure the integrity of the information.

10.1 How to save file

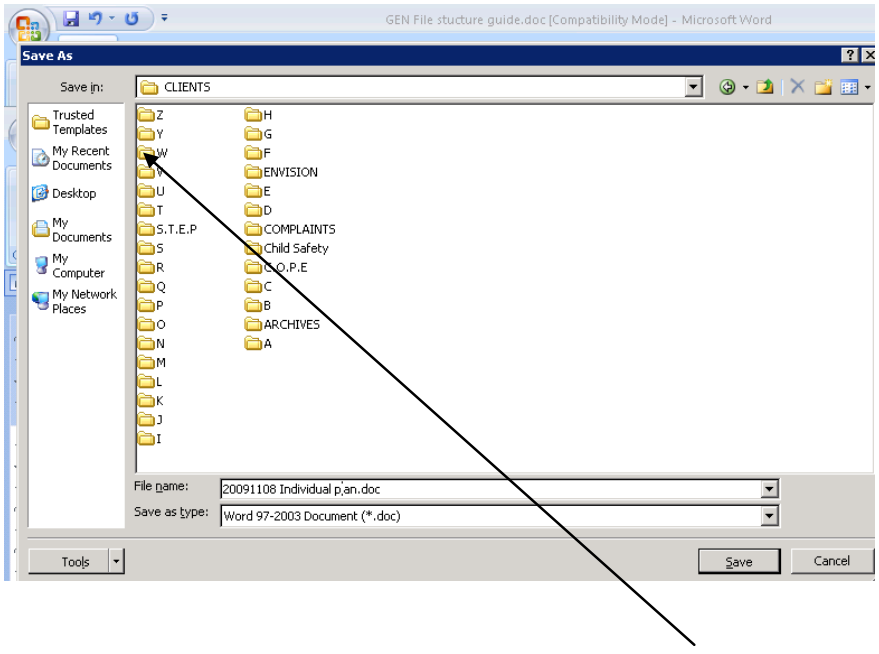
When you want to save a file, open the file and:

Step 1: Click on the Office Button on the top left-hand corner of the screen



Step 2: Click on ‘Save As’

Step 3: Open the ‘Clients’ folder



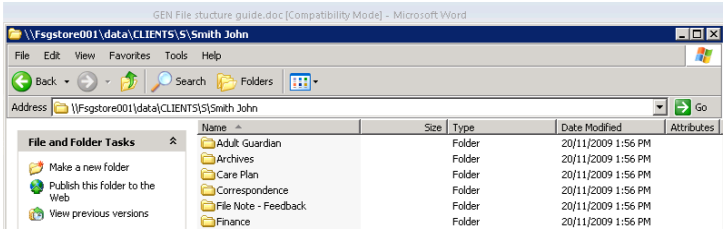
Step 4: Double-click on the first initial of the person's surname (or the specific program file first if relevant).

Step 5: Double-click on the person's name

Step 6: Select the appropriate sub-folder and press 'Save'.

10.2 Creating a sub-folder

If the person's sub-folder does not exist, email it@fsg.org.au and request the creation of the folder.



Usually sub-folders will be created for each person when they are set up by IT. There may be additional folders for specific people, but in general all people will have the following sub-folders:

Public Guardian

Archives

Client Finance

Consent (non medical health)

Correspondence

File Notes – feedback

Finance

Medical – Health

Planning

Profile

You are to email a completed Service delivery history form to it@fsg.org.au when requesting the creation of new folders.

10.3 Scanning documents

The main reason for scanning documents is to be able to save documents containing handwriting e.g. a signature. Other than these, a Word or Excel document may be saved to the person's file. Case notes or file notes do not need to be scanned before saving (unless handwritten). If it is important that a document be protected, saving in PDF may be required.

You are not to scan multiple documents into one file as this makes retrieval very difficult.

If part of the person's profile is updated, scan the relevant section and save into the 'profile' folder.

10.4 Naming files

Date

File names are required to be preceded by this format YYYYMMDD e.g. 20101127.

This date is not the date the document was filed—it is the date the document was created e.g. if a profile dated 3/5/10 is filed on 10/05/10, the file name commences with 20100503.

This ensures the file is in chronological (or date) order. This is important when deciding whether files are to be archived later.

Initial

The next part of the file name is the person's initial, this assists with the identification of misfiled information. Note that the person's name may be the carer for some programs—not the service recipient.

This part of the file name is the initial of the person in whose file the information will be saved e.g. John Smith would be JS—not necessarily the initials of the person to whom the information pertains e.g. a client's carer.

Example 1: Information about an interview with Francis Smith (the service recipient's carer) is being saved to John Smith's file (the service recipient) so the file name would be 20100607 JS Francis Smith interview.

Example 2: Information about a conversation with John Brown (the son of a carer) is being saved to Robert Brown's (the service recipient) file so the file name would be 20100607 RB Record of conversation with John Brown.

The document's purpose

The next part of the file should give the file retriever some indication of what the purpose of the document is e.g. 'photo consent', or 'profile section 5 medication'. For example, 20101126 JS Photo consent.

☞ Note:

PRN authorisations should include the medication name in the filename to assist the retriever to find the file easily.

Do not use abbreviations in file names as this makes saving faster but slows retrieval.

Do not scan multiple documents into one file as this makes naming, and therefore retrieval, very difficult.

10.5 Understanding the content of sub-folders

The following describes the content of each person's sub-folder. Worker who are unsure of the filing structure should seed assistance to avoid accidently corrupting the filing system.

Public Guardian

All information related to the Public Guardian.

Archives

All superseded documents or those which it is not foreseen will need to be retrieved e.g. old menu plans.

Client Finance

All documents relevant to the person's finances e.g. client contribution forms, client plans.

Consent (non medical health)

All consent forms other than medical and health related e.g. Consent and release form, exchange of information form.

Correspondence

Unless specifically relevant to other folders this file contains:

- letters to customers or on their behalf to others
- notifications to other FSGA programs/departments e.g. maintenance service request, hazard report
- letters from other people or organisations which are related to the person
- requests by people to access information.

File note – feedback

The 'file note – feedback' folder contains feedback records, file notes, case notes, incidents (under a sub-folder) and grievances. Or if these are held centrally on the grievance or incident file, a notation should be on the file that these documents exist elsewhere.

Approved program-specific documents are used to record information, which may be required for later reference, and then filed in the person's file.

Finance

This file contains finance information which is not of a personal nature e.g. awake hour claim forms and funding information.

Medical Health

This file contains all relevant medical information—but not profile updates as these should be in the profile folder. This folder will include PEG feeding records, epilepsy management plans, diabetes consultation forms, PRN authorisations, medication consent forms and medication charts.

Planning

This folder should contain:

- individual plans or program-specific plans
- service delivery history forms
- risk management forms
- advocate nomination forms
- DSE preference forms
- menu plans
- positive support plans
- service exit forms
- carer support plans
- fact sheet sign off forms.

Profile

This contains the person's profile and snapshot and/or may contain program-specific files containing personal information which is necessary to provide a service e.g. Legacy Care Plan.

Note: Other than the 9 client folders listed above, you must not create other folders.

Should you wish to identify program-specific documents, the program name is included in the file description e.g. 20101126JS **Lakeview** individual plan review.

10.6 Documents under development

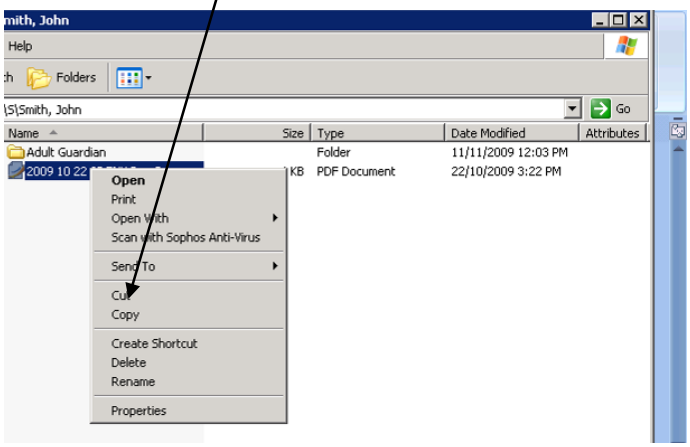
Files which are under development should not be saved on the person's central file; these should be in program files until ready to be dated and saved on the file.

10.7 Moving folders to the archive folder

There are different ways to move files to the person's archive folder. The simplest way is described here:

Step 1: Right click on the file you wish to archive

Step 2: Click on cut



Step 3: Open the person's archive folder (note that this is a sub-folder of the person's folder—not to be confused with the archive folder which holds all the files of customers who are no longer receiving a service).

Step 4: Right click on the mouse and click on 'paste'.

10.8 Creating customer folders

IT or delegated workers are responsible for creating folders. When requested to create a folder, the archive folder(s) is first searched. If the new customer has previously been an FSGA customer (verified with the date of birth), the folder is moved, by IT workers, from the archive folder back into the active folder. All the person's files are moved to the archive sub-folder, thus creating a new folder, with access to previous files.

Persons' folders are named with the surname first and the given name separated by a comma e.g. Smith, Jane. If it is necessary to identify a carer with a different surname than that of the customer, this name may also be added e.g. Smith, Jane – Brown, Mary Carer.

The Service delivery history form is placed on the person's file.

11.0 Using and disclosing personal information

The intent is that FSGA will generally use and disclose a person's personal information only in ways the person would expect.

You should be aware of any service-specific exemptions as detailed in the Privacy Act 1988 - Sect 7B and other legislation governing the release of information e.g. the *Disability Services Act*.

11.1 Considerations before release

11.1.1 All workers

You should always consider whether FSGA can achieve its purpose without disclosing personal information. FSGA should normally only use personal information if it is related to the purpose for which it was collected and within the reasonable expectations of the person to whom the information relates.

You must take such steps (if any) as are reasonable in the circumstances to ensure the quality of personal information when using or disclosing personal information. Procedures required to check the quality at the time of disclosure are:

- check that the information has been updated within a timeframe suited to the purpose and information being released e.g. information related to a person's short-term medical condition may need to be updated before release
- de-identify any information which is not relevant e.g. workers' names may be de-identified in situations where adverse effects to that worker may be an outcome
- take reasonable steps to ensure opinions are accurate, which could include:
  - ensuring the opinion is from a reliable source
  - providing the opinion to the individual before it is used or disclosed
  - clearly indicating on the record that this is an opinion and identifying who has formed that opinion
- only use or disclose so much of the personal information as is relevant to the purpose of a particular use or disclosure.

11.2 Personal information released for a secondary purpose

The Coordinator/Manager is responsible for ensuring a detailed record of the disclosure for a secondary purpose is placed on the person's file.

If information is to be used or disclosed for a new purpose that is not the primary purpose of collection, check the quality of the data having regard to that new purpose before the use or disclosure e.g. data collected on a person's allergies for the purpose of providing a community access service may need updating if the secondary purpose of the data disclosure is to provide a professional medical service to the individual.

Disclosure of personal information for a secondary purpose may be legal if:

- the person consented (refer to 8.0 Understanding consent) to a secondary use or disclosure
- the person would reasonably expect the secondary use or disclosure, and that is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose
- the secondary use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order or a 'permitted general situation' exists in relation to the use or disclosure of the information by FSGA e.g.:
    - lessening or preventing a serious threat to life, health or safety
    - taking appropriate action in relation to suspected unlawful activity or serious misconduct
    - locating a missing person
    - reasonably necessary for establishing, exercising or defending a legal or equitable claim
    - reasonably necessary for a confidential alternative dispute resolution processes.
- the secondary use or disclosure of the information if a 'permitted health situation' exists in relation to the use or disclosure. FSGA may disclose health information about an person for a secondary purpose if:
    - the person receives a health service from FSGA
    - the recipient of the information is a responsible person for the individual
    - the person is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure
    - FSGA is satisfied that either the disclosure is necessary to provide appropriate care or treatment of the person, or the disclosure is made for compassionate reasons

- the disclosure is not contrary to any wish expressed by the person before the person became unable to give or communicate consent of which FSGA is aware or of which FSGA could reasonably be expected to be aware

- the disclosure is limited to the extent reasonable and necessary for providing appropriate care or fulfilling compassionate reasons.

11.3 Disclosure of funding and statistical data

Personal information may be used for funding and statistical purposes. They may be released to government funding bodies to enable the collection of information regarding demographics (for example age, location, disability, language, nationality) and service received. The ensuing reports assist the government in determining consumer/community group needs and planning for the future.

The National Disability Agreement (NDA) National Minimum Data Set (NMDS) is:

- a set of nationally significant data items that are collected in all Australian jurisdictions (i.e. states, territories and Commonwealth)

- an agreed method of collection and transmission, which facilitates the annual collation of nationally comparable data about services funded under the NDA.

The Executive Manager of Customer Relations and Compliance Centre is responsible for ensuring that the collection of FSGA data occurs.

11.4 Recording consent to release customer personal information

Consent is required from the customer (or decision maker) for personal information to be obtained from or released outside of the organisation. In situations where it is not expedient to gain written consent directly from a person, the worker witnessing the verbal consent may keep a record that they witnessed the gaining or withdrawal of consent.

The worker keeping this record or receiving the record from the person is responsible for placing the record on the person's file.

The Coordinator/Manager is responsible for ensuring it is reviewed annually by delegated workers.

If at any time the person who gave consent wishes to withdraw written consent, they may initial against the information descriptor to indicate withdrawal of consent, or if verbal withdrawal of consent is given, the worker witnessing the withdrawal of consent may complete the form to indicate withdrawal of consent.

The updated record is placed on the person's file.

11.5 Recording release of information to enforcement bodies

When personal information is used or disclosed in accordance with enforcement-related activities e.g. police, FSGA must make a written note of the use or disclosure (APP 6.5):

- the date of the use or disclosure
- details of the personal information that was used or disclosed
- the enforcement body conducting the enforcement related activity, and
- if FSGA used the information, how the information was used
- if FSGA disclosed the information, who it disclosed the information to (this may be the enforcement body or another entity)
- the basis for FSGA's 'reasonable belief'. This will help assure us that this exception applies, and it may be a useful reference if the entity later needs to explain the basis for its belief.

This requirement does not apply where a law prohibits the making of such a record.

11.6 Recording disclosure of information

Workers must keep a record when they disclose personal information to another APP entity because, on request, reasonable steps must be taken to notify another APP entity of a correction made to personal information that was previously provided to that entity, unless it is impracticable or unlawful to do so (refer to the APP 13.2). FSGA should inform the individual that they can make such a request, at the time, or as soon as practicable after a correction is made. These records are to be placed in the most appropriate location e.g. on a customer's file.

11.7 Releasing information to third party contractors

A 'use' may extend to providing personal information to a contractor. This must only occur if:

- the contractor only uses the information to perform the contract and
- under the terms of that contract FSGA retains control over the information (for example, an obligation of confidentiality is placed on the personal information or an obligation to abide by the Privacy Act and FSGA is able to terminate the contract if there is a breach).

11.8 Legal obligation to provide information

Ref: https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/businesses/centrelink-has-requested-information-from-my-organisation-about-an-individual-will-i-breach-the-privacy-act-if-i-give-out-this-information

If Centrelink sends FSGA a formal written notice requesting certain information, and the notice states that FSGA is required to provide the information by law, and also states the law under which FSGA is required to provide that information, then FSGA will need to comply.

FSGA may be asked to disclose information to other Commonwealth or State/Territory agencies or authorities from time to time. Again, where a legal obligation to provide information is specified in a formal written notice, FSGA will need to comply.

It is very important that if unsure whether a requested disclosure is required by law, the worker should speak with the government department or authority that is seeking the information. They must be able to explain to the worker which law requires them to meet their request.

A record should be made of disclosure as detailed in 11.5 Recording release of information to enforcement bodies.

12.0 Understanding consent

Consent means ‘express consent or implied consent’. The four key elements of consent are that:

- it must be provided voluntarily
- the person must be adequately informed of what they are consenting to
- it must be current and specific, and
- the person must have the capacity to understand and communicate their consent.

Express consent is given explicitly, either orally or in writing (unless otherwise specified in FSGA procedure). This could include a handwritten signature or an oral statement to signify agreement.

Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the person and FSGA.

FSGA should not assume that a person has consented to a collection, use or disclosure just because the collection, use or disclosure appears to be advantageous to that person. Similarly, FSGA does not establish implied consent by showing that, if the person knew about the benefits of the collection, use or disclosure, they would probably consent to it.

Generally, it should also not be assumed that a person has given consent on the basis that they have not objected to a proposal to handle personal information in a particular way. It is likely to be difficult for FSGA to demonstrate that a person's silence was intended to mean consent.

In particular, consent may not be implied if the person's intent is ambiguous, such as where there is reasonable doubt about the person's intention.

For example, a person's intention may be ambiguous where FSGA implies a person's consent from their failure to opt out. Use of an opt-out mechanism to infer a person's consent will only be appropriate in limited circumstances. FSGA will be in a better position to establish the person's implied consent the more that the following factors, where relevant, are met:

- the option to opt out was clearly and prominently presented
- it is likely that the person received and read the information about the proposed collection, use or disclosure, and about the offer to opt out
- the person was aware of the implications of not opting out
- the option to opt out is freely available and not bundled with other purposes
- receiving and exercising the option to opt out is easy to take up. That is, it involves little or no financial cost to, or effort from, the person
- the consequences of failing to opt out are not serious
- if the person opts out later, they are fully restored, to the circumstances that they would have been in if they had opted out earlier.

FSGA should generally seek the express consent of a person where it proposes to handle the individual's sensitive information, given the greater impact that the collection, use or disclosure of sensitive information may have on the privacy of the person.

FSGA should implement procedures and systems to obtain and record consent, which leave no doubt that consent has been given, either on the basis of the express consent of a person, or clearly implied consent from the conduct of the person.

Consent is voluntary if a person has a genuine opportunity to provide or withhold their consent. Consent is not voluntary where there is duress, coercion or extreme pressure that would equate to an overpowering of will.

Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the person, if they choose not to consent

- the seriousness of any consequences if a person declines to consent
- any adverse consequences for family members or associates of the person if the individual declines to consent.

Bundled consent refers to the practice of ‘bundling’ together multiple requests for a person’s consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not. This practice has the potential to undermine the voluntary nature of the consent.

A person must be aware of the implications of providing or withholding consent for example, whether the person is able to access a service if they do not consent to FSGA collecting a specific piece of personal information. FSGA must give information directly to the individual about how their personal information is to be handled, in a way that the individual understands. Particularly, the information should be written in plain English, without legal or industry jargon.

FSGA should generally seek consent from a person at the time that it proposes to collect, use or disclose that individual’s personal information. FSGA should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to ‘all legitimate uses or disclosures' (see also, discussion of ‘bundled consent’ above).

An individual may withdraw their consent at any time. If they do, FSGA would no longer be able to rely on consent having been given when dealing with the individual’s personal information.

An individual must have the capacity to consent. This means that the individual is capable of understanding the issues relating to the decision to consent, including the effect of giving or withholding consent, forming a view based on reasoned judgement and communicating their decision. If FSGA is uncertain as to whether an individual has capacity to consent, it should not rely on any statement of consent given by the individual.

Issues that could affect an individual’s ability to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because they are unconscious or in severe distress, or
- limited understanding of English.

FSGA should consider whether these issues could be addressed by providing the individual with appropriate support to enable them to exercise their capacity. If an individual does not have capacity to consent and consent is required, FSGA should consider who can act on the individual's behalf. Options include:

- a guardian
- someone with an enduring power of attorney
- a person recognised by other relevant laws, or
- a person who has been nominated in writing by the individual while they were capable of giving consent.

Where an individual lacks the capacity to consent, they should be involved, as far as is practical, in any decision-making process. To the extent possible in the circumstances, FSGA should ensure that privacy issues are discussed with individuals who have impaired decision making capacity in a way that is understandable and comprehensible.

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. FSGA will need to determine whether a young person has the capacity to consent on a case-by-case basis.

As a general principle, a young person has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example if the child is very young or lacks the maturity or understanding to do so themselves.

13.0 Managing the quality of personal information for customers of disability, aged and mental health services

FSGA takes reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, up to date, complete, relevant and the quality of the information is appropriate for the purpose of the use or disclosure.

13.1 Personal information review

Customers of disability, aged and mental health services information may be located in print outs and on TRACCS. The Coordinator is responsible for scheduling regular reviews of customers' personal information and reviewing information as emergent needs arise. Customers' personal information is to be updated at least annually or as required to ensure the information is up to date.

At the time of disclosure, the Coordinator should ensure that, having regard to the purpose of using or disclosing the personal information, it is not only accurate, up to date and complete, but that it is also relevant.

If information is to be used or disclosed for a new purpose that is not the primary purpose of collection, assessing the quality of the data having regard to that new purpose before the use or disclosure.

13.2 Creating quality customer records

Direct service employees are responsible for fully recording significant issues and events for placing promptly on customers of disability, aged and mental health services files. This includes ensuring all file entries include the name, designation and signature (for hard copies) of the person making the entry (refer also to Managing Incidents Procedures).

All workers who are responsible for creating customers' records are required to:

- use plain English which the reader will understand, without using jargon or acronyms
- be open about the information collected and kept on the file
- only include information that is directly relevant to the service/s being provided and limited to that which is necessary to record
- convey respect and support for the person and significant others e.g. their family or carer
- positively describe the person
- avoid using negative language or imply negative views about the person, their reactions, attitudes, family, other services, friends, community etc.
- avoid attributing blame, responsibility or fault
- avoid expressing personal opinions or views—if recording a professional opinion relevant to their role, they are required to make the reasoning clear.

13.3 Professional reports

All professional reports should contain information, which is:

- accurate and without discrepancies—the report should not contain any discrepancies, omissions or mistakes, as the report could be used as evidence in court or the basis of decisions. Providing incorrect or false information particularly for malicious intent is

considered misconduct. If it is determined that a worker knowingly gave false information, their employment may be terminated.

- objective and an unbiased perspective—a professional report should not contain any emotional content; such as “I believe he was sorry…”, “I felt he was uneasy…”, “I did not like…”. The facts should be stated.

- concise and to the point—frivolous and irrelevant information should not be included in the report. Reports need to contain sufficient information regarding the incident in a concise manner.

- descriptive—the report should contain enough visually descriptive detail to enable the reader to gain an accurate and very clear understanding of the incident

- legible to the reader—all reports should be easily understood, by everyone who has access to them. Too many ideas should not be presented at once, however enough information is required in order that the reasons behind what has occurred are clear.

- professional, including using correct professional language—correct grammar and politically correct language should be used. Slang words or derogative remarks should not be used.

14.0 Securing personal information

FSGA plans and implements reasonable steps, based on a clear understanding of the terms ‘misuse’, ‘interference’, ‘loss’, ‘unauthorised access’, ‘modification’ or ‘disclosure’. The terms ‘misuse’, ‘interference’, ‘loss’, ‘unauthorised access’, ‘modification’ and ‘disclosure’ are not defined in the Privacy Act so it is appropriate to refer to the ordinary meaning of these words. FSGA should also consider the meaning of these terms as clarified by courts from time to time, and in other consumer law contexts.

14.1 All workers

You must:

- adhere to systems in place to protect the security of information stored electronically e.g. passwords are not to be given to another person and you are required to change your password if you think it has been compromised

- secure both open and closed hardcopy files in a locked area or a central filing area; not removing hard copies of person’s files from the office, unless being archived or transferred to another service site

- use secure locked bags to maintain the integrity and privacy of the information when personal information (including snapshots) is to be carried external to FSGA

- only fax personal information in exceptional circumstances and only when the privacy of the information is guaranteed (i.e. the receiving unit can guarantee the security and privacy of the information) and with the authorisation of the Coordinator/Manager
- only provide employees/volunteers/contractors with information that is required for them to perform their duties
- de-identify emails containing personal information unless sending via *secure email*[1] and only send to relevant health care partners who have secure email locations and only with Coordinator/Manager authorisation
- treat all personal information in a way that respects persons' rights to privacy and dignity. This includes ensuring a person's information is not discussed:
    - with people other than those who need to know
    - in front of the person to whom the information pertains—if they are not included in the discussion
    - in front of other people who do not need to know
    - without the appropriate consent (refer to 12.0 Understanding consent)
    - in public
- only raise issues which are appropriate and relevant e.g. in the context of handovers, professional supervision or debriefing
- place all wastepaper, on which there is any personal information or data, in a secure location for disposal (under no circumstances should this type of waste paper be thrown away with normal rubbish in the wastepaper bins)
- control all risks to a breach of privacy associated with using recycled paper
- ensure the immediate removal of printed material containing personal information from printers or photocopiers
- log off when leaving your desk if the privacy of electronic personal information is deemed to be at risk e.g. if a visitor is sitting in front of the computer.

[1] The method required to securely transfer confidential data electronically is via public key infrastructure (PKI). Digital signatures and encryption of data is required when electronically sharing confidential information of this nature.

14.2 IT Manager

You are responsible for the security of personal information held electronically by having in place the security systems for protecting information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails).

You are responsible for ensuring, as far as reasonably practicable, that FSGA complies with legislation related to new IT options e.g. cloud computing, which typically refers to a technical arrangement under which users store their data on remote servers under the control of other parties and rely on software applications stored and perhaps executed elsewhere, rather than on their own computers.

14.3 Privacy Advisor

You are to have a commitment to conducting a Privacy Impact Assessment for any new project in which personal information will be handled, or when a change is proposed to information handling practices[2]

14.4 Emailing personal information

Workers who email personal information to unsecure locations are responsible for de-identifying personal information before it is emailed or faxed i.e. identify the information with a code developed by using the person's initials (and the date of birth if there is any chance of misinterpretation of the person's identity e.g. Jane Gloria Smith born 31/12/56 would have the code JGS311256—not the person's name). Inform the addressee verbally of the identity of the person and the relevant identifier. To avoid confusion or mix-ups, ask the addressee to repeat back the information. Also ensure the addressee is informed of their confidentiality obligations by including in the email or fax the following text:

"This information has been sent only for the use of the person to whom the correspondence is addressed. If sent electronically, this information may be printed once only for the use of the addressee only. Once printed, material may not be copied without prior permission from the sender. Whilst in use, all electronic and hardcopy information is to be held securely and free from access to any persons other than the addressee. Where hard copies of personal information are physically transported, and there is a risk of privacy being breached, securely locked bags are to be used to maintain the integrity and privacy of the information.

Once information is no longer required, the addressee is required to dispose of the information securely i.e. hardcopies are shredded or electronic material is deleted.

[2] Further information about Privacy Impact Assessments is contained in OAIC, *Privacy Impact Assessment Guide* (2010), <www.oaic.gov.au>.

Any deviation from these requirements will be a breach in legislative requirements and may result in disciplinary action."

14.5 Receiving personal information via external mail

Workers who are aware that they will receive personal information via external mail should inform the sender to clearly mark the envelope with the word 'Private'. This ensures that the mail will be forwarded unopened to the addressee.

15.0 Destroying or de-identifying personal information

15.1 Statutory obligations

Once personal information is no longer needed for any purpose for which the information may be used or disclosed under the APPs it is to be destroyed or de-identified. This requirement does not apply where the information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the information.

15.2 Hardcopy

Information held in hard copy, must not be disposed of through garbage or recycling collection, unless the information had already been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding[3]

15.3 Electronic storage

It is not possible for FSGA to irretrievably destroy personal information held in electronic format for technical reasons because deleting the personal information is impossible without also deleting other information, held with that information, which FSGA is required to retain.

Therefore the information is put 'beyond use'.

This means that FSGA:

- will not attempt, to use or disclose the personal information
- will not give any other entity access to the personal data

[3] See the *Information security management guidelines* of the Australian Government *Protective Security Policy Framework* (PSPF), Attorney-General's Department Protective Security website, <www.protectivesecurity.gov.au>. Although the PSPF only applies to Australian Government agencies, the examples may also be relevant to organisations in complying with APP 11.2.

- surrounds the personal information with appropriate technical and organisational security. This includes, at a minimum, access controls together with log and audit trails, and

- commits to take reasonable steps to irretrievably destroy the information if, or when, this becomes possible.

16.0 Providing access to personal information to the individual

Written requests should be sent on the Access to personal information request form to the privacy@fsg.org.au.

16.1 Identifying the person

When a request for access to personal information is received, FSGA must be satisfied that the request is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent. The minimum amount of personal information needed to establish an individual's identity should be sought. Where possible, the information should be sighted rather than copied or collected for inclusion in a record.

For example, in a face-to-face dealing with an individual FSGA may be able to record that an identity document was sighted without copying the document. In a telephone contact it may be adequate to request information that can be checked against records held by FSGA, such as a date of birth or address.

16.2 Processing the request for an individual to access their personal information

FSGA will endeavour to provide access in a manner that is as prompt, uncomplicated and inexpensive as possible.

16.3 Grounds on which access can be declined

APP 12.3 lists ten grounds on which FSGA can decline to give access to personal information. It is nevertheless open to FSGA not to rely on any such ground and to provide access upon request, unless disclosure is prohibited. Before relying on any of these grounds FSGA should consider whether editing some information would enable access to be provided (for example, removing personal information about another person).

The grounds, which are considered separately below, are:

- FSGA 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 (APP 12.3(a))
- giving access would have an unreasonable impact on the privacy of other individuals (APP 12.3(b))
- the request for access is frivolous or vexatious (APP 12.3(c))
- the information relates to existing or anticipated legal proceedings between FSGA and the individual, and would not be accessible by the process of discovery in those proceedings (APP 12.3(d))
- giving access would reveal the intentions of FSGA in relation to negotiations with the individual in such a way as to prejudice those negotiations (APP 12.3(e))
- giving access would be unlawful (APP 12.3(f))
- denying access is required or authorised by or under an Australian law or a court/tribunal order (APP 12.3(g))
- FSGA has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to FSGA's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter (APP 12.3(h))
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 12.3(i))
- giving access would reveal evaluative information generated within FSGA in connection with a commercially sensitive decision-making process (APP 12.3(j)).

16.4 Timeframe for responding to a request for access under APP 12

APP 12.4(a) (ii) provides that FSGA must respond 'within a reasonable period after the request is made'. FSGA must respond by giving access to the personal information that is requested or by notifying its refusal to give access. Factors that may be relevant in deciding what is a reasonable period include the scope and clarity of a request, whether the information can be readily located and assembled, and whether consultation with the individual or other parties is required. However, as a general guide, a reasonable period should not exceed 30 calendar days.

16.5 How access is to be given under APP 12

FSGA must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP 12.4(b)). The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record.

Factors relevant in assessing whether it is reasonable and practicable to give access in the manner requested by an individual include:

- the volume of information requested – for example, it may be impracticable to provide a large amount of personal information in person or by telephone
- the nature of the information requested – for example, it may be impracticable to give access to digitised information in hard copy
- any special needs of the individual requesting the information – for example, it may be reasonable to give information in a form that can be accessed via assistive technology where this meets the special needs of the individual; or to send information by email or give it over the telephone if it is difficult or costly for the individual to access the information in person.

16.6 Access charges under APP 12

FSGA cannot impose upon an individual an application charge for requesting access to personal information. FSGA may, however, impose a charge for giving access to requested personal information, provided the charge is not excessive (APP 12.8). Items that may be charged for include:

- costs in searching for, locating and retrieving the requested personal information, and deciding which information to provide to the individual
- costs in reproducing and sending the information
- costs of postage or materials involved in giving access
- costs associated with using an intermediary.

16.7 Giving written notice where access is declined, or not given in the manner requested under APP 12

APP 12.9 provides that if FSGA declines to give access, or to give access in the manner requested by the individual, FSGA must give the individual a written notice setting out:

- the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds for refusal

- the complaint mechanisms available to the individual, and
- any other matters prescribed by regulations made under the Privacy Act.

The reasons for refusal should explain, where applicable:

- that FSGA does not hold the requested information
- the ground of refusal — for example, that FSGA is required or authorised by a law referred to in the written notice to decline access
- that access cannot be given in the manner requested by the individual, and the reason why
- that the steps necessary to give access in a way that meets the needs of FSGA and the individual under APP 12.5 are not reasonable in the circumstances.

The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:

- a complaint should first be made in writing to FSGA
- FSGA should be given a reasonable time (usually 30 days) to respond
- a complaint may then be taken to a recognised external dispute resolution scheme
- lastly, a complaint may be made to the Information Commissioner (s 36).

17.0 Referee reports

Unsuccessful job applicants or those awaiting the outcome generally should be able to get access to those reports.

To make sure FSGA gets the best person for the job, FSGA wants referees to provide accurate reports. An inaccurate referee's report could affect employment opportunities. As far as possible, the information FSGA collects should be accurate, complete and up to date. In most circumstances, the Privacy Act gives applicants the right to access and correct all the personal information an organisation holds about them. This would include a referee's report.

18.0 Correcting personal information

18.1 FSGA correction obligations

FSGA must take reasonable steps to correct personal information it holds, to ensure it is accurate, up to date, complete, relevant and not misleading, having regard to the purpose for which it is held.

APP 13 also sets out other minimum procedural requirements in relation to correcting personal information. FSGA must:

- upon request by an individual whose personal information has been corrected, take reasonable steps to notify another organisation of a correction made to personal information that was previously provided to that other organisation
- give a written notice to an individual when a correction request is declined, including the reasons for the refusal and the complaint mechanisms available to the individual (APP 13.3)
- upon request by an individual whose correction request has been declined, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out of date, incomplete, irrelevant or misleading (APP 13.4)
- respond in a timely manner to an individual's request to correct personal information or to associate a statement with the information (APP 13.5(a))
- not charge an individual for making a request to correct personal information or associate a statement, or for making a correction or associating a statement (APP 13.5(b)).

18.2 Correcting at the individual's request

18.2.1 Contact to request correction of personal information

Written requests to correct personal information should be sent to privacy@fsg.org.au.

18.2.2 Grounds for correcting personal information

Grounds for correcting personal information include inaccuracy (if it contains an error or defect), out of date (if it contains facts, opinions or other information that is no longer current), incomplete (if it presents a partial or misleading picture, rather than a true or full

picture), irrelevant (it is irrelevant if it does not have a bearing upon or connection to the purpose for which the information is held) and misleading (it is misleading if it conveys a meaning that is untrue or inaccurate or could lead a reader into error). For examples of grounds for correcting personal information refer to http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/draft-australian-privacy-principles-guidelines/draft-app-guidelines.

18.2.3 Requesting further information from the person

If FSGA requires further information or explanation before it can be satisfied that personal information is faulty, FSGA should clearly explain to the individual what additional information or explanation is required or why FSGA cannot act on the information already provided. FSGA should also advise where additional material may be obtained. The individual should be given a reasonable opportunity to comment on the refusal or reluctance of the entity to make a correction without further information or explanation from the individual.

FSGA should also be prepared in an appropriate case to search its own records or other readily-accessible sources to find any information in support of, or contrary to the individual's request. For example, FSGA could take into account a finding of an Australian court or tribunal relating to the personal information that has a bearing on whether it is or is not faulty.

18.2.4 When correction is declined

If FSGA declines to correct personal information as requested by an individual, FSGA must give the individual a written notice setting out:

- the reasons for the refusal, except to the extent that it would be unreasonable to do so
- the complaint mechanisms available to the individual, and
- any other matters prescribed by regulations made under the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

The reasons for refusal should explain, where applicable:

- that FSGA does not hold the personal information that the individual wishes to correct
- that FSGA is satisfied that the personal information it holds is accurate, up to date, complete, relevant and not misleading having regard to the purposes for which it is held, or

- that the steps necessary to correct the information as requested are not reasonable in the circumstances.

The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:

- a complaint should first be made in writing to FSGA
- FSGA should be given a reasonable time (usually 30 days) to respond
- a complaint may then be taken to a recognised external dispute resolution scheme, and
- lastly, that a complaint may be made to the Information Commissioner (s 36).

Other information can also be included in the notice advising an individual that a request to correct personal information has been declined. The individual can be advised of the right under APP 13.4 to request FSGA to associate a statement with the personal information.

18.2.5 Access charges under APP 13

FSGA cannot impose upon an individual:

- an application charge for requesting correction of personal information
- a charge for correcting the personal information or for associating a statement with the personal information (APP 13.5(b)).

19.0 Closure of files for customers using disability, aged and mental health services

19.1 When a person is no longer receiving an FSGA service

Step 1:

The Coordinator updates the Service delivery history form on the person's file and sends a copy to it@fsg.org.au to request that the person's file is moved to archive.

Step 2:

After scanning those documents which require archiving, the Coordinator is responsible for ensuring all hardcopy documents containing personal information are destroyed in a manner which makes retrieval impossible.

Step 3:

The person's folder is moved by IT to the archive folder, providing there are no other services being received by the person. The person's folder name is preceded with the date the person exited FSGA in the format of YYYYMMDD.

19.2 When a customer returns to FSGA

Should the person commence receiving FSGA service whilst the information is still in archives, the folder name is amended by IT (i.e. the preceding date is removed) and the folder moved back to the 'current' folder. The Coordinator is responsible for placing a new Service delivery history form on the person's file and archiving the old form i.e. moving the superseded form to the person's sub-folder named *archive*).

20.0 Ensuring personal information is beyond use

Personal information retention is in accordance with relevant legislation/funding agreement governing the funding body. Coordinators/Managers are to advise IT when files are no longer to be kept. Examples of legislated record keeping follows:

20.1 Disability Services Regulation

Records are to be kept for at least 7 years.

The records required to be made and kept by a funded non-government service provider under section 214 of the Act which will/may contain customer personal information are the following:

- the name, address and telephone number for each of the provider's consumers
- the name, address and telephone number for the person nominated as the emergency contact for each of the provider's consumers
- documents relating to written complaints made to the provider about the delivery of disability services by the provider
- details of each conflict of interest arising under the provider's conflict of interest policy, including how the conflict was dealt with
- copies of documents given by the provider to the chief executive relating to incidents that have happened in the provision of disability services by the provider
- data collected for the National Minimum Data Set

- a record of the financial delegations and internal controls in place under the financial delegations policy
- the financial records required to be kept by the provider under the funding agreement entered into by the provider.

20.2 Aged Care Act

Records are to be retained for the period ending 3 years after the 30 June of the year in which provision of the care ceased.

Records which will/may contain customer personal information which are required to be retained in accordance with the Aged Care Act are:

(a) assessments, appraisals for classification and classifications of care recipients

(b) individual care plans for care recipients

(c) medical records, progress notes and other clinical records of care recipients

(d) schedules of fees and charges (including retention amounts relating to accommodation bonds) for previous and current care recipients

(e) agreements between care recipients and the approved provider

(f) accounts of care recipients

(g) records relating to the approved provider meeting prudential requirements for accommodation bonds

(h) records relating to the payment and repayment of accommodation bonds (including periodic payments)

(i) records relating to care recipients' entry, discharge and leave arrangements, including death certificates where appropriate

(j) records relating to a determination that a care recipient is a care recipient with financial hardship

(k) records of the amount of accommodation charge paid or payable to the approved provider by care recipients

(l) records of the amount of accommodation charge refunded by the approved provider in relation to care recipients who paid an accommodation charge for a period during which they were charge exempt residents

(m) up-to-date records of:

i) the name and contact details of at least 1 representative of each care recipient, according to information given to the approved provider by the care recipient, or by the representative; and

ii) the name and contact details of any other representative of a care recipient, according to information given to the approved provider by the care recipient, or by the representative.

21.0 Community Visitors

Community visitors conduct unannounced visits so they can see the standard of support provided on a typical day at a site.

Community visitors have the legislative authority to:

- access all areas of a site
- require workers to answer questions
- request documents related to the support of residents
- make copies of relevant documents and
- confer alone with residents or workers.

22.0 WH&S inspectors

An inspector can enter places as specified at Inspectors, entry powers and conduct - Workplace Health and Safety Queensland with or without the consent of the person with management or control of the place and without prior notice to any person unless the place is used only for residential purposes and does not involve the storage of dangerous goods, high risk plant or access to a workplace.

It is an offence to obstruct, threaten or interfere with an inspector who is exercising their powers.

23.0 Police right to personal information

Police have a right to ask for a person's name and address in many situations, which are listed in a number of different laws. Some of the most important occasions listed in the PPRA include when:

- the person has been found committing an offence
- the person is 'reasonably suspected' of committing an offence
- police think the person may be able to assist in the investigation of an indictable offence or act of domestic violence
- the person has been given an order to stop making noise or to stop being a nuisance
- the person is in control of a vehicle that is stopped on a road; or

- police are trying to enforce another specific law.

Police can also ask for proof of identity where it is reasonable in the circumstances.

If the person declines to give their name and address when police have a right to ask for it, and they do not have a reasonable excuse for declining to cooperate, they will be committing an offence and could be charged.

Giving a false name or using someone else's name could result in more serious charges.

Police can remain in a person's yard and enter their home against the person's wishes, of course, if they have a warrant (for example, a search warrant allowing them to search the place, or a warrant for a person's arrest) or if they have some other specific, legal right to remain there. If the police tell the person that they have a warrant that justifies their entry to their home, the person should insist on seeing it. Police are required to give the person a copy of the warrant.

Police can conduct searches for evidence without a warrant when a police officer reasonably believes that evidence of a particular offence will be destroyed or concealed if they do not enter and search the relevant place immediately. This power applies to indictable (serious) offences, offences involving gaming, betting, explosives, drugs, weapons or possessing alcohol in restricted areas.

24.0 Electronic monitoring of residents using accommodation services

Also refer to: http://www.justice.qld.gov.au/__data/assets/pdf_file/0007/258361/emi-report.pdf

24.1 Assessing the need

Prior to implementing electronic monitoring, the need to use electronic monitoring must be fully assessed.

The use of electronic monitoring must relate to a lawful purpose that is directly related to the function of FSGA.

FSGA also considers whether electronic monitoring, including being considered for use, is the best way to achieve this purpose e.g. even while the electronic monitoring may be considered necessary, it may not be necessary to actually keep the audio or visual recordings and 'live' monitoring may suffice.

FSGA will complete a needs assessment for each resident who will be considered as a subject for electronic monitoring.

FSGA will seek the resident's (or decision maker's) views about electronic monitoring e.g. preferences about how the electronic monitoring should be utilised, such as location and the opportunity for the resident to activate or deactivate the monitor.

The need and method of monitoring must be reviewed at least 6 monthly or as emergent needs arise.

24.2 Gaining consent

Informed consent must be obtained before electronic monitoring commences (refer to 12.0 Understanding consent). This is to include any residents who will be incidentally or unintentionally monitored.

Consent for electronic monitoring will be recorded on the Electronic monitoring collection notice. As with all consent this may be withdrawn at any time and must be current (no more than 6 months old). '

25.0 Privacy Commissioner's contact details

Post: GPO Box 5218 Sydney NSW 2001*	**Location:** Office of the Australian Information Commissioner Level 3, 175 Pitt Street Sydney NSW 2000
Fax: +61 2 9284 9666	**Email:** privacy@privacy.gov.au**
Telephone Enquiries: 1300 363 992	**TTY:** 1800 620 241

26.0 Privacy procedure review

Privacy procedures will be reviewed in accordance with the Controlled Document Management policy at least 2-yearly.

27.0 Privacy breach

There are four key steps to consider when responding to a breach or suspected breach:

Step 1: Contain the breach and do a preliminary assessment

Step 2: Evaluate the risks associated with the breach

Step 3: Notification

If the data breach is likely to involve a real risk of serious harm to individuals, or receive a high level of media attention, inform the Executive Services Officer who may contact the OAIC. The OAIC may be able to provide guidance and assistance.

Step 4: Prevent future breaches

These steps are covered in more detail at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

APPENDIX A – Frequently asked questions

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

1. Can I decline to provide our APP procedures in a requested format?

Yes FSGA can decline to provide a copy of its APP Privacy Policy in a particular form if it would not be reasonable in the circumstances to meet the request. For example, doing so may be unduly costly or unnecessary in light of other steps taken by FSGA to make its policy publicly available and accessible. Before declining a particular request, you should consider any reasons given by the body or person for requesting the policy in a particular form, any special need the requester may have to be given access in a particular form, whether FSGA has unique or unusual information handling practices, and whether the nature, volume or sensitivity of the personal information held by the FSGA makes it appropriate that its policy is made available in additional forms.

Australian Privacy Principle 2 – Anonymity and pseudonymity

1. Can I insist that people provide identifying information?

Yes, whilst APP 2 provides that 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, that principle does not apply in relation to a particular matter if it is impracticable for FSGA to deal with individuals who have not identified themselves or used a pseudonym (APP 2.2(b)).

Australian Privacy Principle 3 – Collection of solicited personal information

1. How do I know what personal information I can collect?

FSGA must only collect personal information which is reasonably necessary for 'one or more of FSGA's functions or activities' (APPs 3.1 and 3.2). Factors that may be important in determining whether a collection of personal information is reasonably necessary for a function or activity include:

- the primary purpose of collection
- how the information will be used in undertaking a function or activity of FSGA (e.g. collection on the basis that information may become necessary for future activities would not be reasonably necessary)
- whether FSGA could undertake the function or activity without collecting that information, or by collecting a lesser amount of personal information.

The following are instances in which the Privacy Commissioner has previously ruled that a collection of personal information was not reasonably necessary for an entity's function or activity:

- a job applicant being asked to advise if they had suffered a work-related injury or illness, when this was not relevant to the position being advertised
- a person applying to open a bank account being asked to complete a standard form application that included a question about marital status, when this had no bearing on the applicant's eligibility to open an account
- a medical practitioner photographing a patient for the patient's medical file, when this was not necessary to provide a health service.

- Other examples of personal information collection that may not be reasonably necessary for an APP entity's functions or activities include:

- collecting personal information about a group of individuals, when information is only required for some of those individuals
- collecting more personal information than is required for a function or activity – for example, collecting all information entered on a person's drivers licence when the purpose is to establish if the person is aged 18 years or over
- collecting personal information that is not required for a function or activity but is being entered in a database for future reference.

2. Is it okay to collect information from a decision maker if the person does not have capacity to provide the information?

Yes, APP 3.6 provides that FSGA 'must collect personal information about an individual only from the individual', unless it is unreasonable or impracticable for FSGA to collect personal information only from the individual

Australian Privacy Principle 6 – use or disclosure of personal information

1. What personal information can be required or authorised by law?

FSGA may use or disclose personal information for a secondary purpose if the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b)).

Examples of where FSGA may be required or authorised by law to use or disclose personal information include where:

- a warrant, order or notice issued by a court requires FSGA to provide information, or produce records or documents that are held by FSGA

- FSGA is subject to statutory requirements to report certain matters to agencies or enforcement bodies, for example specific financial transactions, notifiable diseases and suspected cases of child abuse.

2. Can FSGA give personal information without consent in an emergency medical situation?

FSGA may use or disclose personal information for a secondary purpose where:

- FSGA reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, and
- it is unreasonable or impracticable to obtain consent (s 16A(1)(item 1)).

3. When consent is required should it be written or verbal?

Express consent is given explicitly, either orally or in writing (unless otherwise specified in FSGA procedure). This could include a handwritten signature or an oral statement to signify agreement.

4. What if Disability Services requests information?

The Disability Services Act states:

223 Power to require information or documents

(1) The chief executive may give notice to a funded non-government service provider requiring the service provider to give the chief executive, within a stated reasonable time, information or a document relating to the provision of disability services to consumers of the service provider.

(2) The funded non-government service provider must comply with the notice.

(3) For a requirement to give a document, the service provider may comply with the requirement by giving a copy of the document certified as a true copy of the document.

4. What are my obligations under the Aged Care Act to release information to the Department?

The Aged Care Act states:

90-4 Meaning of monitoring powers

(1)The following powers are monitoring powers:

(a) any of the following in relation to premises:

(i) to search the premises;

(ii) to take photographs (including a video recording), or make sketches, of the premises or any substance or thing at the premises;

(iii) to inspect, examine and take samples of, any substance or thing on or in the premises;

(iv) to inspect any document or record kept at the premises;

(v) to take extracts from, or make copies of, any document or record at the premises;

(vi) to take onto the premises any equipment or material reasonably necessary for the purpose of exercising a power under paragraph (i), (ii), (iii), (iv) or (v);

(b) in relation to a thing that may afford evidence of the commission of an offence against this Act, the powers in subsection (2);

(c) in relation to documents or records at premises, the powers in subsections (3) and (4).