

PRIVACY, DIGNITY and INFORMATION

BACKGROUND INFORMATION

This document formally recognises each resident's right to privacy and confidentiality. It is updated to incorporate regulatory changes made periodically.

Confidentiality relates specifically to the protection of private information acquired through the service and the policy is consistent with the Freedom of information Act, 1982 plus legislative updates.

The right to privacy and confidentiality will be protected and promoted. Staff, however, must give due credence to duty of care responsibilities and an adequate level of supervision will be provided, where necessary.

The facility will ensure that, wherever possible and within the constraints of safe and effective program provision, this policy will be enacted in the following ways:

1. Residents are not watched, listened to or reported upon without consent unless it concerns good care management.
2. The dignity and privacy of each resident is protected during any personal care activity.
3. Intrusion into residents' activities is minimal and their right to privacy is respected.
4. Residents are not the focus of uninvited public attention.
5. Residents' personal property will be respected by all individuals. All care will be taken by staff when handling belongings but no responsibility will be accepted for their safekeeping.
6. Phone calls and visits can be taken in private, where physical layout permits.

7. Personal mail is received by the resident promptly.
8. Residents have access to, and control over, their own money, with support as necessary. If they are incapable, management will discuss the situation with family.
9. Residents are able to choose whether or not to discuss their feelings, relationships or other aspects of their private lives.
10. Management and staff demonstrate their commitment to treating residents with respect.
11. Staff interact with residents in a manner which reinforces the resident's self esteem.
12. Staff are sensitive in discussing an individual's personal details with any other party, including amongst other staff.
13. Written information about a resident is limited to what is relevant and necessary to that resident's involvement with the facility.
14. Use of any information is limited to the resident and staff who need to use it, and it is stored securely and accessible only to staff.
15. Residents are aware of the information kept about them and their written/verbal permission will be sought prior to releasing any information.
16. A record is kept of the type of information given, and to whom it was designated.
17. Staff refrain from engaging in gossip or unnecessary discussion about residents and/or their families. However, professional feedback and information sharing about residents is welcomed.
18. Where appropriate, residents will be assisted to understand this policy.
19. Staff are also encouraged to knock on bedroom doors before entering; and being aware that other people could be hearing your conversation when you are discussing a resident with a colleague.

Privacy officer

A Privacy Officer has been appointed. This is the Chief Executive Officer. For operational purposes she has delegated to a number of key staff, mainly in general administration and care administration. The privacy officer has overall responsibility for staff training, dealing with complaints and inquiries and monitoring the performance of the privacy policy and procedures.

Privacy audit

A privacy audit will be conducted from time to time, under the auspices of quality improvement processes. This includes how information is collected, stored, destroyed, disseminated and the security of information so it is not passed on inappropriately.

Open and transparent management of personal information

There are requirements called Australian Privacy Principles (APPs). They require the organisation to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs. This will have an impact on organisational information systems (paper and computer); collection methods and staff training.

Unsolicited information

If we receive unsolicited information, then we are required to “de-identify or destroy the information as soon as practicable”. For example, if a prospective resident in filling out a resident agreement accidentally provides personal records not relevant to their care or financial position, then this would constitute unsolicited information and should be destroyed.

Notification of the collection of personal information

The facility will provide additional information to an individual such as who can access the information; how the individual can access and correct their personal information and how the individual can make a complaint about a breach of the APPs.

An entity (e.g. doctor or carer) will only be able to collect sensitive information if the individual consents and the information is reasonably necessary for the entity's functions.

Direct marketing

This facility does not provide information to direct marketing, except for internal use of mailing addresses for newsletters and other relevant community information relating to resident care.

Security of information

Computer server systems are in place to provide security, including back-up to prevent loss of data; firewalls to prevent unauthorised external access; and various passwords and computer partitioning to manage internal access to certain types of information, e.g. personal details.

The facility has an internal IT co-ordinator to ensure smooth operation of the computer systems; and an IT contractor also has a continuous monitoring role to prevent interference or modification. This also protects information from computer viruses and virtual attacks.

INFORMATION SYSTEMS

The following is a guide to understanding how information should be treated according to the legislation. Only some staff will have responsibility, but all should be aware of the details.

Internet and email policy

It is the responsibility of staff, contractors and volunteers of Dorothy Impey Home to use of the internet and email services in a manner that is lawful, ethical, economical and efficient. Personal use of the internet is permitted where it does not impact on the normal execution of a person's duties or the business of the Home. This includes the use of the Internet and Email through internet and email accounts and electronic equipment, including mobile devices such as smart phones and tablets. Social media access such as Facebook and Twitter is not permitted on the premises.

Breaches and enforcement

Internet usage is automatically monitored by the network operating system, which includes a record of access and usage of individual networked machines.

Any employee who knowingly violates or otherwise abuses the provisions of this policy may be subject to disciplinary action.

The Home reserves the right to place any user under direct surveillance to ensure policy compliance. Such a right will only be exercised at the direction of the CEO and the user will be informed of such surveillance.

All staff, contractors and volunteers making use of the Home's internet and email services should be aware that they do not have the same rights to privacy as they would if using a private device. In other words, these services belong to the Home and not you.

Operational storage

Documents should be stored where it is most logical to keep them. Hard cover folders, appropriately labelled front and side, are normally used to store them for operational purposes. Work in progress is recommended to be contained in a manilla folder with the item written in pencil on the front (so the cover can be reused later).

Length of storage

Documents are stored in operational areas while they are still being used. Occasionally, there should be a review and cull of old documents, and these should be disposed of, or filed appropriately. We advocate the use of special storage areas for old documents that can demonstrate continuous improvement, e.g. old forms that are no longer used because they have been redefined, superseded or no longer in use.

Documents pertaining to past residents should be bundled together and put into archives in case there is ever a need to refer to them.'

Legal documents, financial records, reports, etc. should also be separately archived for at least seven years.

Document retention

Case Records relating to residents receiving residential aged care services where the resident dies whilst receiving care must be kept for 10 years after the death of the resident or last access on behalf of the resident. If the resident does not die when leaving the home, the case records must be kept for 15 years after the resident left or last access on behalf of the resident. Accounting records to be retained and then destroyed after 7 years.

Access

The service area that uses the documents has the access and accountability. Staff from other service areas should request access as a matter of courtesy. Human Resources records (pay documents, etc.) is confidential with limited access to most staff; ditto financial details and some strategic and legal documents.

On a daily basis, the Chief Executive Officer is the deciding authority on who can see defined documents. Legal issues can arise re confidentiality, privacy, and commercial information. If Freedom of Information matters arise, the CEO may seek legal advice re access. Residents (or their representatives); staff, and authorised people (e.g. accreditation assessors) who have concerns about access should follow the guidelines outlined in conflict resolution documents and the policy on handling grievances.

Accountability

The CEO; service staff who have been delegated responsibility; and the development manager are designated as the people accountable for the accuracy, appropriateness, timeliness and appearance of documentation used in this facility.

Normally, the computer copy is seen as the latest edition of a document. Hard copies of most computer documents will normally be stored in appropriate folders in various operational areas. Staff are encouraged to write on these documents as a means of having meaningful updates, or speak to the development manager re designing new forms, and writing or editing documents.

Disposal

Printed documents, i.e. paperwork normally generated internally, are handled in a variety of ways once they outlive their usefulness.

If it has a resident's personal details or has technical details of a confidential business nature, the paper should be put through a shredder, or at least torn into small pieces by hand if a shredder is not available.

Any other general material or photocopied material should be placed in wastepaper baskets for normal disposal.

Documentation that may be required for cross-checking or emergency back-up, or comes under the scrutiny of accreditation auditing, should be filed in suitable storage containers or binders and stored in a safe place, e.g. basement archive storage.

RESIDENT VIDEO SURVEILLANCE

The facility may have occasion to use video surveillance, either in rooms for specific care situations, e.g. palliative, or in corridors to manage falls, behaviour or residents who wander at night. The following must occur

1. The camera is only to be used for the specific purposes mentioned above.
2. The monitor can only be viewed in a restricted area, e.g. general office where only staff have access.
3. A permission form must be signed by each resident at entry. In addition, there will be a prominent sign in an appropriate position warning visitors there is video surveillance.
4. If a camera is used in a bedroom for care monitoring purposes, e.g. assessment and palliative care, then a specific permission form must be signed by the next of kin.
5. The monitor and/or room camera will be switched off if it is considered inappropriate to view certain things which may be happening in the room at a given time, e.g. medical examination; toileting, etc.
6. The CEO is the person with final responsibility for camera placement, under advice from key staff.
7. Any hidden cameras not authorised by the CEO will be removed if found. This is in the interest of privacy concerns for the resident and staff. If a family is concerned about care and treatment behind closed doors, then they should discuss the situation with management. If this is not satisfactory, families can always access the Aged Care Complaints Commission.

Other things to consider . . .

The dignity and privacy of each resident is to be respected. This means . . .

1. Each resident is to be treated with respect.
2. There should be a private and secure space to store belongings.
3. One person's belongings must not be used by another without permission.
4. Activities of a personal nature should be able to be carried out in private.
5. Personal information should be kept in confidence.

Some practical ways of showing dignity and privacy include:

1. Knocking and waiting before entering a person's room.
2. Using a person's belongings only for that person.
3. Inviting a person to join activities instead of telling them.
4. Providing privacy for residents.
5. Supporting a person with eating difficulties as tactfully as possible.
6. Accepting that a person may like to organise his or her belongings as that person wishes – given safety considerations for both resident, visitors and staff.

Actions to be taken to support privacy in a facility include . . .

1. Be aware of policies and procedures to place more emphasis on privacy.
2. Discuss any issues of privacy at staff meetings.
3. Value and respect the personal privacy of the residents.
4. Be aware of the physical environment so that handovers and other private conversations are not overheard.