|  |  |
| --- | --- |
| **POLICY NO & NAME:** | **0010 - RECORDS MANAGEMENT POLICY** |
| **APPROVED BY:** | **Bec Symes, CEO** |
| **DATE CURRENT POLICY APPROVED:** | 22/01/2019 |
| **REVISION DATE/S:** | 22/01/2019 |
| **DATE CREATED:** | 22/01/2019 |

**POLICY STATEMENT**

A well maintained records management system supports the delivery of quality centred services by Greendale Community. Greendale Community acknowledges and respects the privacy and confidentiality of every individual and is committed to complying with all applicable privacy and public records keeping provisions.

Legislation applicable to record keeping and privacy and confidentiality include:

* Public Records Act 1973 (Vic)
* Evidence Act 2008 (Vic)
* Evidence (Miscellaneous Provisions) Act 1958 (Vic)
* Crimes Act 1958 (Vic)
* Information Privacy Act 2000 (Vic)
* Freedom of Information Act 1982 (Vic)
* Health Records Act 2001 (Vic)
* The Privacy Act 1988
* Australian Privacy Principles 2014
* OH&S Act 2004.

Please refer to Greendale Community Privacy and Confidentiality Policy (007) as this policy is closely aligned with the Records Management Policy (010).

**SCOPE & PURPOSE**

The purpose of this policy is to ensure secure collection, recording and updating of information, access to the use of records, security of records and storage, transport and archiving of personal, sensitive and health information of Greendale Community service users, families and friends, employees, potential employees, volunteers, students and the community.

**Record management:**

* Recording
* Storage
* Access and security

**DEFINITIONS**

**Record** is any document within the meaning of the Evidence Act 2008 (Vic) including, written documents, anything with marks / symbols or perforations having a meaning for persons qualified to interpret them, anything with sounds, images which can be reproduced and maps, plans, photographs or drawings.

1. **Collection of Records**

Greendale Community collects service user, employee, students and volunteer information and records.

Service user records and information is collected, recorded and kept for the purpose of:

* Service user care and support: records provide a case history and a holistic picture
* Accountability: evidence of Greendale Community’ response to a service user’s need and funders requirements
* Service improvement: records/data/information can assist with improving services

All service user records must be protected under the Victorian Health Records Act 2001.

Employee, student and volunteer records and information is collected, recorded and kept for purposes such as:

* General HR purposes such as bank details, criminal records, medical certificates
* Incident and accident reports and WorkCover documents
* Supervision and support
* Professional development

Information is to be collected in a sensitive way and in accordance with service policy and procedures documents and will only be used for the primary purpose intended.

Greendale Community will request information from the service user or, with the knowledge of the service user, from their authorised representative. Service user consent will be obtained and documented prior to another source being contacted for relevant information.

Greendale Community is committed to ensuring that all records are accurate, up to date, complete and not misleading. Employee, volunteers, students and service users may request the correction of information or have their dissent regarding any of their personal information recorded.

**Employee Records** consists of Personal Employee or Sensitive and Health Information contained in any records, documents, files and reports that relate to a Greendale Community employee, potential employee, volunteer or student.

Records/files can take many forms besides those often considered as formal.

For example, diary/log entries, a verbal recollection, comments and notes made in communication books or meeting minutes can all be classified as records.

**Service user records** consist of all documents, files and reports that relate to a Greendale Community service user

**Storage of records**

Greendale Community will ensure that:

* Records are kept in appropriate conditions and protected from known risks, deterioration, and unauthorised access
* Records can be efficiently retrieved
* A maintenance program and disaster plan are in place

Electronic records are stored securely with appropriate backup and disaster recovery systems in place.

Hard copies should be stored in secure locations and free from deterioration.

Records should have a file path name / storage location on it, where possible, for ease of access and retrieval. This will depend on security systems in place / authorised access.

Greendale Community uses the following service user (case management information and service user referral) and employee management systems: CRISSP, IRIS, Carelink and Chris21.

Retention and disposal. Any information relating to service users, employees, volunteers or students, such as correspondence or reports, that are not required to be filed, must be destroyed via the confidential document disposal bin located at the Greendale office and Warrnambool office.

When an employee, volunteer, student or most service users exit or complete their service provision with Greendale Community, their file and records will be closed and archived for a period of at least 7 years. After this time the file and records may be shredded or securely destroyed.

In line with DHHS requirements, records for out of home care service users are kept indefinitely at Greendale Community Head Office, Albert St. Geelong West.

Greendale Community also keeps electronic copies of autism assessment reports indefinitely as families may request copies at a later date.

**Access and security of records**

Greendale Community will ensure that records can be accessed not only for administrative and service user management purposes but also as required under applicable legislation such as the Information Privacy Act 2000, the Health Records Act 2001 and the Freedom of Information Act 1982.

* **Access to Service user Information**

Therapy & Inclusion Support Services (T&ISS) and Respite, Recreation & Family Support Services (RR&FS) service users are provided with copies of assessments and reports produced by agency employees. Copies of assessments or reports, Greendale Community has obtained from other professional services for Accommodation & Support Services service users, are provided upon request.

Requests to view a service user’s individual file are to be made through the appropriate program manager.

If the program manager does not approve the release of information, the reasons for this will be provided to the person requesting information and the service user and/or family/advocate/carer have the right to use the agency grievance procedure to have the decision reviewed.

If an NDIA delegate (i.e. an NDIA employee) requires a Greendale Community employee / the Greendale Community organisation to provide information under section 55 of the NDIS Act, the delegate must issue a written notice which specifies:

* the nature of the information or document that is required to be given or produced
* how the person is to give the information or produce the document
* the period within which the person is to give the information or produce the document to the NDIA
* the officer to whom the information is to be given or the document is to be produced
* that the notice is given under s.55 of the NDIS Act.

The period specified in the notice must be at least 14 days beginning on the day on which the notice is given. The notice may require the person to give the information by appearing before a specified officer to answer questions. If the notice requires the person to appear before an officer, the notice must specify a time and place at which the person is to appear. The time must be at least 14 days after the notice is given (see NDIS Operational Guideline – Information Handling – Collecting, Accessing and Recording Protected Information (Dec 2013)**.**

* **Obtaining Consent to access service user, employee, student and volunteer Files and Records for an Audit Process**

Greendale Community will ensure all service users, employees, students and volunteers are informed, in writing, of forthcoming audits. If an individual does not want their files accessed during an audit process can record this on the reply section of the audit information letter. Program Managers are responsible for ensuring the “non-consent to access files” reply is attached to the individual’s files.

* **Limits on the Disclosure of Service user Information**

Service users or their family requiring access to their own personal information on file or in storage, must contact the Service Manager to make access arrangements. Greendale Community may impose a charge upon the individual to cover the cost of verifying a request for information and locating, retrieving and reviewing any material requested. All requests will be responded to within 30 days of receipt. Greendale Community may request Photo Identification prior to access.

If service user information is required to be collected from other parties, Greendale Community will act to ensure the service user, and or family, is, or has been, made aware of the requirement to do so, and their written consent or documented verbal consent is obtained prior to releasing any information.

Greendale Community is not permitted to release:

* Medical letters, as these are the property of the treating doctor, or
* Incident Reports as these are a reporting requirement to DHHS and access must occur through the Freedom of Information Act.

**Security**. Access to information is for authorised employee for legitimate business / service delivery purposes only. Information is to be treated in the strictest of confidence and is not divulged unless for legitimate and legally permissible purposes.

Paper based record management system / files to which access is restricted must be kept securely, e.g. in a safe locked filing cabinet.

Electronic records and shared drives have user logon profiles and the process of restricting access to electronic files / records is authorised and implemented when the logon is set-up.

Staff are **not** to store any service user or staff sensitive or identifiable data in either OneNote or OneDrive – this includes multimedia content such as images and videos.

**Greendale Community Privacy Policy and statement. Greendale Community ensures that information about privacy and confidentiality is included in individual service agreements, service user information package and Greendale Community websites.**

**For detailed information, see Greendale Community Privacy and Confidentiality Policy No 007.**

**RESPONSIBILITIES**

Even though records and files may be created about an individual associated with Greendale Community, such as a service user, employee, volunteer or student etc, their records and files are legally owned by the organisation. Greendale Community recognises that, with this ownership, comes responsibility for the handling, treatment and access entitlements of the information.

Greendale Community will explain to service users, employees, students and volunteers why information is collected and recorded at the time of collection.

If personal information is required to be collected from other parties, Greendale Community will act to ensure the employee, volunteer or student is, or has been, made aware of the requirement to do so.

Greendale Community acknowledges its responsibilities in protecting records with any personal information it has collected and, or has in its keeping, from misuse, modification, loss or unauthorised access and will take all reasonable steps to do so.

At such time that files, records or information are no longer required, Greendale Community take all reasonable steps to destroy or de-identify them.

Employees are required to sign-off that they will read and abide by Greendale Community policies incl. the key HR policies which includes Privacy & Confidentiality Policy as part of their contract

Employees, volunteers and students must respect the confidentiality of service users at all times. Service user files and any information relating to service users, must be stored in a lockable cabinet at all times and must not be removed from the workplace, where it is stored, without authorisation from the relevant Program Manager, and, whenever possible, in a locked case/satchel.

When service user files have been authorised for removal from the workplace, they should be de-identified if at all possible and kept in the locked boot of a vehicle, whenever possible.

Filing cabinets must be locked by the last employee to leave the service area each day.

Only Greendale Community employees with appropriate clearance have access to service user files and reports stored on computer or the central database, i.e. Carelink+ and Chris21.

Program Managers are responsible for ensuring that employees, volunteers, students and service users who have exited their programs have their records and files archived and stored in a lockable location.

Employees leaving Greendale Community are responsible for complying with the Privacy Act and Australian Privacy Principles for deleting, disposing off or returning any service user information and records they may have in their possession. This includes their photos or information in their personal mobile phones, computers etc.

They are also responsible for returning anything that may belong to Greendale Community, such as keys, I.D. Photos etc.

Aged Care Facility documents are held on each section of the facility, in a locked cabinet, or behind a locked door. The most recent documents are kept for easy access, while the previous volumes of service user histories are kept in an off site storage area with comparable security.

**REFERENCES**

|  |  |  |
| --- | --- | --- |
|  | Reference: | Public Records Act 1973 (Vic)  Evidence Act 2008 (Vic)  Evidence (Miscellaneous Provisions) Act 1958 (Vic)  Crimes Act 1958 (Vic)  The Information Privacy Act 2010  Freedom of Information Act 1982 (Vic)  Health Records Act 2001 (Vic)  The Privacy Act 1998  Australian Privacy Principles 2014  OH&S Act 2004  The Information Privacy Act 2009  The Disability Act 2006  Australian Privacy Principles 2014  The OH&S Act 2004  Fair Work Act 2009  Child Wellbeing and Safety Act 2005  NDIS Act 2013  Aged Care Act 1997 |
| • | Industry Standard Reference | National Standards for Disability Services  Community Common Care Standards  National Quality Framework  Children’s Services Regulations 2009  The Early Years Learning Framework for Australia (Early Years Learning Framework)  Child Safety Standards  NDIS Operational Guideline – Information Handling – Collecting, Accessing and Recording Protected Information (Dec 2013)  Australian Aged Care Quality Agency-Accreditation Standards |