|  |  |
| --- | --- |
| **POLICY NO & NAME:** | **007 PRIVACY & CONFIDENTIALITY 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**

Greendale Community acknowledges and respects the privacy and confidentiality of every individual and is committed to complying with all applicable privacy provisions.

Greendale Community provides services in accordance with:

* Greendale Community Employees Code of Conduct (includes volunteers and students)
* The Information Privacy Act 2010
* Australian Privacy Principles (2014)
* Privacy and Data Protection Act 2014
* Victorian Health Records Act 2001
* Freedom of Information Act 1982
* Fair Work Act 2009
* Occupational Health & Safety Act 2004
* NDIS Act 2013
* Privacy Act 1988

and, where applicable:

* The Disability Act (2006)
* Aged Care Act 1997
* Department of Human Services Standards
* National Standards for Disability Services
* Home Care Standards
* Specialist Children’s Services Standard 5 – Confidentiality and Privacy
* Australian Government Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) privacy requirements
* Department of Social Services requirements
* Children’s Services Regulations 2009
* Child Safe Standards (Victoria)
* NDIS Operational Guideline – Information Handling – Collecting, Accessing and Recording Protected Information (Dec 2013)

**SCOPE & PURPOSE**

The purpose of this policy is to protect personal, sensitive and health information of Greendale Community service users, families and friends, employees, potential employees, volunteers, students and the community, whilst ensuring the delivery of a quality service.

The policy outlines the following information:

1. The kinds of personal information that Greendale Community collects and holds
2. How Greendale Community collects and holds personal information
3. The purpose for which Greendale Community collects, holds, uses and discloses personal information
4. How an individual may access personal information held by Greendale Community, about the individual, and seek correction of such information
5. How an individual may complain about a breach of the Australian Privacy Principles, or registered APP code (if any), that binds Greendale Community and how Greendale Community deals with enquiries or complaints from individuals about Greendale Community’ compliance with the Australian Privacy Principles.
6. Whether Greendale Community is likely to disclose personal information to overseas recipients.

Greendale Community will collect only information that is reasonably necessary for one or more of its functions/activities or services/programs or if this is required by Australian law or a court/tribunal order.

Greendale Community Privacy and Confidentiality policy is available on the Greendale Community’ website (in different languages through the translation service and AAA) and in hard copy format on request at any service location.

**DEFINITIONS**

**Individual**: Greendale Community service users, families and friends, employees, potential employees, volunteers, students and the community.

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

* Personal and emergency contacts and next of kin details.
* Financial affairs, superannuation details, taxation and banking information.
* Hours of work, salary and wages.
* Training, development and performance records.
* Disciplining, resignation or termination.
* Contracts, agreements, terms and conditions of employment.
* Correspondence.
* Photographs.
* Computer files and email.

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

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

**Employee Sensitive and Health Information** consists of any records, documents, files and reports that relateto a Greendale Community **employee, potential employee, volunteer or student, such as:**

* Racial or ethnic origin.
* Political opinions or membership of a political association.
* Membership of a professional or trade association or trade union.
* Religious or philosophical beliefs or affiliations.
* Sexual preferences or practices.
* Criminal records and information, note that these documents may be destroyed, following assessment, in accordance with the relevant Program Funding Body requirements.
* Information regarding their health or disability.
* Their expressed wishes about their future provisions of health services.
* A health service provided, or to be provided or information provided about health services.

Any of the above information may be recorded in Medical Certificates, Workcover Documents, Professional Development and Support Session notes, Education Background Information or Resume Affiliations and must be protected under the Victorian Health Records Act 2001.

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

* Personal and emergency contacts and next of kin details.
* Racial or ethnic origin
* Religious or philosophical beliefs
* Case notes
* Tape, DVD and video recordings
* Computer files and email
* Photographs
* Financial details
* Health Care Plans and other health information
* Behaviour and Active Support Plans
* Incident reports
* And other written records

All service user records must be protected under the Victorian Health Records Act 2001 and record management is consistent with the Public Records Act 1973. For details regarding Greendale Community’ record management see Policy No. 2208 Records Management.

**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** acknowledges its responsibilities in protecting 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 made aware of Greendale Community Privacy & Confidentiality Policy during their induction (and need to be fully aware that any employee who fails to comply with this policy may be subject to disciplinary action). Furthermore, employees sign-off in their contract that they will abide by this policy.

When employees, volunteers and students support service users with their personal

care needs they will protect their dignity.

**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 Service 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.

Employees, volunteers and students must not access/view service user files of family members (incl. children, parents or siblings), e.g. protected participants (NDIS definition) as there needs to be a separation between service delivery and the family.

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 and central data / ICT systems such as Carelink+ and Chris21.

Greendale Community **Volunteers** and **Students** are also required to comply with Greendale Community Privacy and Confidentiality Policy. They receive this information and discuss its relevance to their role during their induction.

**Service 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 the Australian Privacy Principles for deleting, disposing off or returning any service user information 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.

**PROCEDURES**

Greendale Community will only collect personal information by lawful and fair means.

**1. SERVICE USER INFORMATION**

**1a Collection of Service User Information**

Greendale Community collects service user information only where it is necessary for:

* the delivery of effective and efficient service provision to the service user (and his/her family where applicable).
* the mandatory data requirements required by the funding body.

Information will be collected in accordance with service policy and procedures documents and will only be used for the primary purpose intended. If Greendale Community wishes to use or disclose the information for another purpose (secondary purpose) the individual needs to give consent for this.

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.

**1b Access to Service User Information**

Therapy & Inclusion Services, Support Coordination and Respite, and Recreation Support Services and service users in the South West and Western Melbourne 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 & Specialist Support Services service users, are provided upon request.

Any request to view a service user’s individual file are to be made through the appropriate Service Manager.

If the Service 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/carer/advocate have the right to use the agency grievance procedure to have the decision reviewed.

If an NDIA (National Disability Insurance Agency) 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, and
* That the notice is given under section 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)**.**

# 1c Obtaining Consent to access Service User Files and Records for an Audit Process

Greendale Community will ensure all service users are informed, in writing, of forthcoming audits. Service users who do not want their files accessed during an audit process can record this on the reply section of the audit information letter. Service Managers are responsible for ensuring the “non-consent to access files” reply is attached to the service user’s files. The Quality & Service Development Manager keeps a record of all “non-consent” service user information for the audit.

**1d 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 or provided to other parties (incl. health information), Greendale Community will act to ensure the service user, and or family, is, or has been, made aware and consent of the requirement to do so.

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 DET and access must occur through the Freedom of Information Act.

Principles governing the use and disclosure of health information are set out in the Privacy Act under National Privacy Principle 2 which states that an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection except for a number of situations, including where an organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or a serious threat to public health or public safety.

In short Greendale Community staff must not disclose a person’s health information e.g. Hep B and C status or HIV status without consent as universal infection control precautions should provide protection for staff. An exception may occur in a very limited number of circumstances such as: - cases of needle-stick injury where a professional is aware of a patient’s HIV positive status and a health care worker has been exposed in circumstances where there is a real risk of transmission and it is not possible to conceal the identity of the source patient who has refused to consent to disclosure, - provision of medical services in a particular instance of care where there is a need to know the infection status for treatment purposes of benefit to the patient (e.g. in an emergency or if the patient is unconscious). This should not, however, detract from the observance of standard infection-control precautions.

**1e Service user Publicity Participation**

If service users are participating in any promotional material or included in any media releases of whatever form, permission must be obtained in writing from the service user or parents of the service user concerned.

The Chief Executive Officer must also approve the use of service users in such publicity.

**2. EMPLOYEE, VOLUNTEER AND STUDENT INFORMATION**

**2a Recruitment**

Information provided by candidates in recruitment and selection is voluntary.

However, if some of the requested information, such as information required to obtain a Crim Check, is not provided, Greendale Community may not be able to assess an application for employment.

# 2b Obtaining Consent to Access Employee, Volunteer and Student Files Information For An Audit Process

Greendale Community will ensure all employees, volunteers and students are informed of forthcoming audits. Employees, Volunteers and students who do not want their information accessed during an audit process can record this with the HR Manager to be entered into a “non-consent to access files” database. The HR Manager will ensure the non-consent is in the persons file.

**2c Limits on the Disclosure of Employee, Volunteer or Student Personal Information**

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.

Employees, volunteers or students requiring access to their own personal information, must contact the Greendale Community Corporate Services 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 will not provide copies of personal information once collected. Access will be granted by viewing the information on the premises of Greendale Community. The personal Information may not be removed from the premises. Greendale Community may request Photo Identification prior to access.

**2d Greendale Community Employee Records kept by other Groups**

Preschools have the responsibility to ensure the secure storage of Additional Assistants employee information forms kept on their premises.

**2e Employee, Volunteer and Student Publicity Authorisation**

Permission must be obtained, in writing, if employees, volunteers or students are to be used in any promotional material or included in any media releases of any form.

**2f Comment to the Media**

Under no circumstances are Greendale Community Employees, Volunteers or Students to make comment to the media in relation to Greendale Community, service users or programs without prior authorisation from the Chief Executive Officer.

**3. RELEASE OF INFORMATION**

**3a Non Release of Information**

Greendale Community is legally entitled to deny the release of information.

The basis for such a decision would be that:

* the organisation 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
* providing access would have an unreasonable impact on the privacy of other individuals;
* the request for access is frivolous or vexatious;
* the information relates to anticipated or existing legal proceedings and would not be discoverable in those proceedings;
* providing access would reveal the intentions of Greendale Community in relation to negotiations with the individual in such a way as to prejudice those negotiations;
* providing access would be unlawful.

**3b Exceptions for Release of Information Restrictions**

Information may be provided to statutory authorities in circumstances deemed necessary to safeguard the interests of the person concerned.

These exceptions for release of information restrictions, are consistent with The Privacy Act, and, include:

* reporting child abuse to the relevant authority
* the provision of Category 1 and some specified Category 2 Incident Reports to DHHS or DET where a significant incident affecting a service user or members of the public has occurred.
* action which prevents or lessons a serious threat to the life or health of the person concerned.
* where information is ordered to be provided by a court of law.
* Greendale Community has reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
* the use or disclosure is required or authorised by or under law; or
* Greendale Community reasonably believes that the use or disclosure is reasonably necessary for a specified purpose by or on behalf of an enforcement body.

**4. CORRECTION AND ACCURACY OF INFORMATION**

Greendale Community is committed to ensuring that all records are accurate, up to date, complete and not misleading and will take all reasonable steps to ensure this.

Employees, volunteers, students and service users may request the correction of information, or have their dissent regarding any of their personal information recorded.

**5. RETENTION AND DISPOSAL OF PERSONAL INFORMATION**

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 bag located at the Albert Street office.

When an employee, volunteer, student or service user exits or completes 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 will be shredded or securely destroyed. For more details, see Records Management Policy (Policy No 2208).

**6. RESPECTING COMMUNITY PRIVACY**

Greendale Community ensures that members of the community give consent for the use of any photos taken by Greendale Community support Services in promotional materials or media releases.

**7. GREENDALE COMMUNITY PRIVACY STATEMENT**

Greendale Community ensures that information about privacy and confidentiality is included on each service brochure, service user information package and Greendale Community websites.

**8. REQUIREMENTS FOR EMPLOYEES LEAVING GREENDALE COMMUNITY**

In order to comply with the Privacy Act, Employees leaving Greendale Community are required to return, destroy or delete any Greendale Community information they may have in their possession. This includes information stored on their phones and emails etc.

**9. SENDING INFORMATION BY FAX OR EMAIL**

There are risks to privacy in sending information by fax. These include miss dialling the number, people other than the intended recipient reading the information, the information not being authentic or the transmission not being authorised. Where information is being faxed, the fax number should be checked twice. Greendale Community fax proforma is marked private and confidential and includes a privacy statement stating that the recipient should contact Greendale Community immediately if a fax is received in error.

There are also risks to privacy sending information by email. These include misdirection due to error in typing the address and the ease of copying, forwarding, amending or disclosure of the information. If the information is being emailed care should always be taken with the list of addressees. Greendale Community emails contain a privacy statement including the need to contact Greendale Community and immediately delete an email received in error.

**10. COMPLAINTS & NOTIFICATION**

Complaints by any individual about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds Greendale Community are dealt with through the Greendale Community Feedback Compliments and Complaints Policy and Employee, Volunteer and Student Grievance Procedure. Privacy breaches are reported to the relevant funding body.

DHHS and NDIS privacy breaches/incidents need to be submitted to DHHS using the web based Privacy Incident Report eform.

For information: https://dhhs.vic.gov.au/publications/privacy-policy

**The Notifiable Data Breaches (NDB) scheme** requires Greendale Community to notify the Australian Information Commissioner (the Commissioner) about ‘eligible data breaches’. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates. For details see https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

**REFERENCES**

|  |  |  |
| --- | --- | --- |
|  | Reference: | The Information Privacy Act 2010  Privacy and Data Protection Act 2014  The Privacy Act 1998  The Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Privacy Act)  The Victorian Health Records Act 2001  The Disability Act 2006  The OH&S Act 2004  Fair Work Act 2009  Australian Privacy Principles 2014  Freedom of Information Act 1982  Child Wellbeing and Safety Act 2005  Disability Act 2006  Aged Care Act 1997  NDIS Act 2013  Victorian Reportable Conduct Scheme |
| • | Industry Standard Reference: | National Standards for Disability Services  Home Care Standards  Specialist Children’s Services Standards  National Quality Framework  Department of Social Services privacy requirement  Childrens Services Regulations 2009  Child Safe Standards  NDIS Operational Guideline – Information Handling – Collecting, Accessing and Recording Protected Information (Dec 2013) |