CONFIDENTIALITY AND PRIVACY POLICY

Related Quality Frameworks and Legislation:	
Aged Care Quality Standards (ACQS)	Standard 1: Consumer Dignity and Choice
NDIS Quality Standards (NDIS)	Standard 1: Person-Centred Supports
Legislation	Privacy Act 1988 – Part III, Division 2 Australian Privacy Principles Notifiable Data Breaches Scheme http://www.legislation.qld.gov.au

1. Purpose

Gladstone Community Linking Agency (GCLA) is committed to protecting the confidentiality and privacy of personal information which the organisation collects, stores and administers and that persons dealing with us understand our practices in relation to the management of their personal information. Privacy for customers may relate to their physical environment, possessions, physical needs, personal relationships and personal information.

In order to ensure each customer is treated with dignity and respect, GCLA must respect their privacy by ensuring the behavior and interactions of staff do not compromise customers privacy. GCLA customers and paid and unpaid staff have legislated rights to confidentiality and privacy, and to accessing their own records. It is essential to protect and uphold these rights and to act correctly in those circumstances where the right to confidentiality or privacy may be overridden by other considerations.

Personal information, as defined by the Privacy Act 1988, is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

Sensitive information, as defined by the Privacy Act 1988, is information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health, genetic or biometric templates, that is also personal information.

Confidentiality implies the relationship of confidence between an organisation and individuals. Customers disclose private information in a relationship of trust with GCLA.

Privacy protects the access to a person such as being free from public attention and choosing to keep your matters to yourself while confidentiality protects access to your data. It is about not disclosing the information to unauthorised people.

We recognise the rights of customers and employees for GCLA to maintain their privacy and confidentiality and to have their information administered in ways which they would reasonably expect.

GCLA manages all personal information according to law and best practice.

2. Scope

This Policy applies to the Board of Directors, all paid and unpaid staff, students on placement, contractors and consultants who are required to adhere and be guided by this Policy.

3. Policy Detail

Gladstone Community Linking Agency is committed to protecting and upholding the rights of customers, staff and volunteers to privacy and confidentiality. This means that GCLA ensures no personal information about a customer or paid or unpaid staff member is shared with anyone, on purpose or by omission, unless informed consent or in special circumstances where the law allows or dictates an exception such as when a person is a danger to themselves and/or to others.

Health information is one of the most sensitive types of personal information. It is essential that we respect a consumer's right to privacy in how we collect, use and communicate health information. We manage all personal information according to law and best practice.

In order to treat a customer with dignity and respect, we must respect their privacy. We ensure the behaviour and interactions of the workforce and others do not compromise customer privacy. We respect each customer's right to privacy in how we collect, use and communicate their personal information.

Specifically:

- Staff must at the outset, obtain consent to collect and hold customer information. Staff must provide to the customer, or representative, information on the records GCLA holds and how to access their own personal information if they wish.

- Staff must not access customer files unless required to do so as part of their usual duties working with customers. Any customer files held manually or electronically have restricted access to appropriate staff. Customer records are not held in areas or on drives shared with staff or others who are not involved in providing service to the customer.

- All staff, when first employed, must sign an information confidentiality statement about customer information they may be exposed to, during their tenure.

- All staff commit to privacy and confidentiality for each customer when we:
    a. provide support and care to a customer
    b. provide privacy for the customer within their home, room or private areas
    c. provide customers with private and discreet spaces for any discussions regarding a customer's care and service requirements
    d. store a customer's personal information, whether this relates to medical needs or general information.
    e. de-identify information provided to government departments regarding service provision output data

GCLA staff respects our customer's privacy and keeps their personal information confidential by:

1. <u>Seeking customer permission</u>
    - Asking permission from customers before entering their home, room or private areas.
    - Providing privacy to each customer for personal care activities e.g. bathing, toileting, dressing and personal/intimate relationships.
    - Making sure customers have privacy when speaking with visitors and during phone conversations, if the customer or their representative chooses.
    - Not open or read customer mail unless the customer requests this or needs assistance.
    - Treating all information relating to customers confidentially.
        - Not using customer's personal property unless invited to do so as the customer's personal property is their own.
        - Sharing confidential information about the customer, including their records, in a way that maintains the customer's privacy and confidentiality.

- Conducting handovers between shifts in areas where information cannot be overheard by those who should not have access to it. This also applies to information given to health professionals or representatives involved in the customer's care or services.
- Gaining consent from the customer or their representative to share their electronic records or personal information with another service provider or health care professional when a written request to access their records or personal information is received.
- Actively participating in and learning about privacy and dignity.

2. Being careful with how we collect and use customer information
    - The customer shall be asked for consent to collect and share information with relevant professionals for the purposes of their care and informed they can withdraw consent for sharing their personal information at any time.
    - The customer receives a Collection Statement which outlines the types of personal information collected, how it is collected and used, how it may be disclosed and the importance of complete and accurate information.
    - We collect personal information from the customer only, unless they consent to collection from someone other than them, or it is unreasonable or impractical to do so.
    - Staff must not seek more information about the customer than is necessary to provide care and services.
    - Staff do not release customer information to any third party without customer consent. Any customer information is released and/or accessible only to those with a legitimate interest or need as part of their care or service role.
    - Sometimes other personal information must be collected about the customer's families and social relationships, personal interests, skills, behaviour patterns and financial affairs to provide services. If this is required, the purpose of this collection will be clearly explained to the customer or their representative.
    - Staff do not proceed with customer assessment, care and support coordination or planning processes without customer consent. If the customer cannot provide consent due to disability, medical condition or other reason, consent is sought from their representative.
    - Documentation on all customers file notes is written objectively, observing:
        - respect for the customer's feelings and dignity
        - the customer's right to request and have access to their own records
        - freedom of information and court requirements that may subpoena customer files.

3. Advising customers of their right to access their records
    - We inform customers of their right to access their information and remind them from time to time through service reviews and agreement renewals.
    - If an individual requests access to the personal information held about them, or requests changes to that personal information, access is allowed and changes made unless GCLA considers that there is a sound reason under the Privacy Act or other relevant legislation to withhold the information, or not make the changes.
    - Requests for access and/or correction will be required to put in writing and provide proof of identity.
    - Reasonable steps will be provided to access the information requested within 14-30 working days of the request. GCLA may charge reasonable fees to reimburse the cost we incur relating to a customer's request for access to information, including in relation to photocopying and delivery cost of information stored off site.
    - If an individual is able to establish that personal information Gladstone Community Linking Agency holds about her/him is not accurate, complete or up to date, GCLA will take reasonable steps to correct the records.

4. Gaining customer consent to use customer images and audio/visual recordings
    - If an image or audio/visual recording is required for any purpose, we seek consent from the customer or representative.
    - We keep and update a Register of Consents. On receipt of any written notice of withdrawal of consent, we check the register before using any image.
    - If we intend to use customer images in marketing and communication brochures or similar activities, we must obtain written informed consent from the customer or their representative for that situation only. The image cannot be retained for some possible future use.

5. Advising customers of their right to complain of a privacy breach
    - We inform customers about their right to complain about a privacy breach and the process for making a complaint. This information sets out the way that we manage the complaint.
    - Alternatively, the customer may complain to the Office of the Australian Privacy Commissioner within 6 months of the breach.

6. Explaining exemptions for customers rights to access their records and personal information

    A legal requirement to disclose personal information may override the Australian Privacy Principles; this is known as a 'duty of care'. Situations where this may occur include the following:
    - The request does not relate to the personal information of the person making the request;
    - Providing access would pose a serious threat to the life, health or safety of a person or to public health or public safety;
    - Providing access would create an unreasonable impact on the privacy of others;
    - The request is frivolous and vexatious;
    - The request relates to existing or anticipated legal proceedings;
    - Providing access would prejudice negotiations with the individual making the request;
    - Access would be unlawful;
    - Denial of access is authorised or required by law;
    - Access would prejudice law enforcement activities;
    - Access would prejudice an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of GCLA
    - Access discloses a 'commercially sensitive' decision making process or information; or
    - Any other reason that is provided in the Privacy Act.

    If access is denied to information, the reasons for denying the access will be given. Where there is a dispute about a right of access to information or the forms of access, this will be dealt with in accordance with the complaints process.

7. Complying with the requirements for Notifiable Data reaches

    A data breach, according to the Privacy Amendment (Notifiable Data Breaches) Act 2017, occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure and is likely to result in serious harm to any individual affected.

    Examples of a data breach include the following incidents:

    - a device containing customers' personal information is lost or stolen
    - a database containing personal information is hacked
    - personal information is mistakenly provided to the wrong person.

    When GCLA believes, on reasonable grounds, that an eligible data breach has occurred, we must promptly notify the individuals at likely risk of serious harm. The Australian Information Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

The notification to affected individuals and the Commissioner must include the following information:

- the identity and contact details of the organisation
- a description of the data breach
- the kinds of information concerned
- recommendations about the steps, individuals should take in response to the data breach.

Data breaches can cause significant harm in multiple ways. Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

The Notifiable Data Breach (NBD) scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Commissioner of certain data breaches. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm such as an individual can change passwords to compromised online accounts and be alert to identity fraud or scams.

If an eligible data breach occurs, GCLA:

1. Contains the data breach to prevent any further compromise of personal information.
2. Assesses the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
3. Notifies individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.
4. Reviews the incident and consider what actions can be taken to prevent future breaches.

GCLA is accountable to customers and others for building trust in personal information handling throughout the organisation and privacy breaches are taken seriously.

4. Review Processes

Policy review frequency: Every 2 years unless updates are required	**Accountability for review:** CEO
Review process: Delegated responsibility from the CEO to the relevant line manager, according to the Document Review Schedule and process.	
Documentation and communication: Documents are controlled on the Customer Management Record System (CMRS) and updates are communicated to all staff via email and/or staff meetings.	