P01.6 Privacy and Confidential Information

1. What You Need To Know

Twenty10 incorporating GLCS NSW (Twenty10) is committed to protecting and upholding the right to privacy of clients, staff, volunteers, Board members and representatives of agencies we deal with. In particular, the organisation is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

The organisation requires staff, volunteers and Board members to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

Twenty10 follows all State and Federal privacy legislation. The organisation will follow the guidelines of the Australian Privacy Principles in its information management practices.

This policy helps the organisation ensure that:

- it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients, staff, partner organisations, and suppliers
- clients are provided with information about their rights regarding privacy
- clients, staff, volunteers, Board members, partner organisations, and suppliers are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- all staff, Board members and volunteers understand what is required in meeting these obligations.

This policy conforms to the Federal Privacy Act (1988) and the Australian Privacy Principles which govern the collection, use and storage of personal information.

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, to interviews or discussions of a sensitive personal nature, and to proprietary information from partner organisations and suppliers.

Sometimes clients, staff or Twenty10 may send or receive Privileged Communications. Privileged communications are protected from being produced to a Court and other bodies. In order for this protection to be maintained, these communications must remain confidential. This means that disclosure of the communication or its contents, will risk losing the protections.

2. Procedures

2.1. Dealing with confidential information

In dealing with confidential information of clients, staff, volunteers, partner organisations, and suppliers, staff will:

- ensure privacy for clients, staff, volunteers, and Board members when they are being; interviewed or discussing matters of a confidential or sensitive nature
- only collect and store confidential information that is necessary for the organisation to function;
- use fair and lawful ways to collect confidential information;
- collect and/or store confidential information only with consent from an individual;

- ensure that people know what sort of confidential information is held; what purposes it is held for; how it is collected, used, and disclosed; and who will have access to it;
- ensure that confidential information collected or disclosed is accurate, complete, and up-to-date;
- provide access to any individual to review information and correct wrong or out-of-date information about themselves;
- take reasonable steps to protect all confidential information from misuse and loss and from unauthorised access, modification or disclosure;
- destroy or permanently de-identify confidential information no longer needed and/or after legal requirements for retaining documents have expired;
- not make copies of any confidential information, except when required for job duties; and
- not use confidential information collected by the organisation for confidential purposes.

This will not prevent an individual from:

- disclosing information to proper authorities in relation to concerns about improper conduct, breaches of laws or breaches of duty of care;
- providing access for external reviewers to de-identified information for the purposes of formal audit processes;
- making a formal complaint to appropriate authorities about an aspect of the organisation's operation; or
- disclosing any information that they may be required to disclose by any court or regulatory body or under applicable law;

Staff and volunteers are Mandatory Reporters and have a duty of care to breach confidentiality when a child is at risk of harm or where young person is a danger to themselves or others, or where a child is at risk. For more information see [P09.25 Child Protection and Safety].

2.2. Responsibilities for managing privacy and confidentiality

All staff and volunteers are responsible for the management of confidential information to which they have access, and in the conduct of research, consultation or advocacy work. Confidential information is not to be shared outside of the program area in which the staff or volunteer work (e.g. youth client services, QLife, Adult Groups and so on).

The Co-Executive Directors are responsible for safeguarding confidential information relating to staff, volunteers, Board members, contractors, suppliers, and partner organisations. They will be responsible for:

- ensuring all staff are familiar with the Privacy Policy and administrative procedures for handling confidential information;
- ensuring that clients and other relevant individuals are provided with information about their rights regarding privacy; and
- handling any queries or complaints about privacy issues.

The Office and Administration Manager and the Communications and Development Officer are responsible for content in official external communications, and must ensure that:

- appropriate consent has been obtained when including personal information of any individual, including staff and volunteers;

- information provided by other agencies in respect of Twenty10 or its clients, staff or Board members, conforms to the Australian Privacy Principles; and
- the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website.

For more information, refer to [P11.3 External communication].

2.3. Privacy information for clients

At intake, the worker performing intake is to request consent to collect information. Giving this consent is not required to receive services. The intake worker is also to tell new clients what information is being collected, how their privacy will be protected and what their rights are in relation to this information.

When appropriate consent has been given, we can record data in the Australian Department of Social Services (DSS) Data Exchange and the New South Wales Family and Community Services (FaCS) Client Information Management System (CIMS).

In seeking consent to record personal data in the DSS database, we must tell clients that:

- the DSS Data Exchange is hosted by the Australian Department of Social Services
- the organisation uses the Data Exchange as a client management system
- their details will only be provided to our organisation to manage their case
- the DSS use de-identified data from the Data Exchange for policy development, grants program administration, research, and evaluation
- the DSS Data Exchange privacy policy can be accessed from the DSS website and tells them how to access their personal information, seek correction of their personal information, and make complaints about breaches of privacy.

In seeking consent to record personal data in the CIMS database, we must tell clients:

- their personal information will be recorded in a secure client information management system used by the service;
- which service(s) have access to their personal information, under what circumstances and for what reason;
- their right to withdraw or restrict consent;
- how long their information must be stored by law;
- their right under privacy and access laws to access their personal information; and
- how to make a complaint about the service.

Service users can withdraw their consent to data collection at any time. The DSS Data Exchange also allows users to withdraw consent to collecting personal data while still using their de-identified data.

It is best practice to ask for consent from a parent or guardian for service users under the age of 18. However, due to the nature of the work conducted by Twenty10, it may not always be appropriate or necessary to seek consent from their parent or guardian in circumstances where the person under 18 is mature enough to provide consent on their own.

Best practice in health services re: assessing minor's capacity to consent (and, particularly, exclude parents from decisions) is to apply the Gillick Principle - which states: the parental right to make decisions for their minor child terminates if and when the child achieves sufficient

understanding (1) and intelligence (1) to understand what is proposed. The key factors to be considered when determining "Gillick Competence" are:

(a) Minor's age

(b) Minor's maturity

(c) Nature, consequences and implications of the decision

(d) Ability of the child to weigh up nature, consequences and implications

Client Services Staff utilise the Gillick Principle when conducting intake and assessment of a new client to make a decision on a case by case basis regarding consent.

For people with disabilities or other cognitive impairments that could compromise their ability to give consent, it might be appropriate for their consent to be witnessed by a family member or key support person. As per the Montreal Declaration, individuals with disabilities should not be automatically assumed to be completely incompetent to make decisions for themselves and that they too have a right to autonomy and self-determination. If the young person cannot consent themselves, because they lack capacity, then a parent, legal guardian, court/lawyer or guardianship board can do so.

Client Records are kept beyond the period of contact with the organisation in line with legislation.

- Child records will be retained until the client reaches 26 years of age.
- Adult records will be retained for 10 years after last contact.
- The records of deceased child and adult clients will be retained, in accordance with legislative requirements, for 7 years after death.
- Following the expiration of the appropriate record retention period, the paper file will be disposed of through secure waste collection.
- Twenty10 Inc GLCS NSW computer record detailing basic information about the client and relevant details of service delivery will be retained in a secure environment as a permanent service record.
- In the spirit of the NSW Public Health Act 2010, the Commonwealth Privacy Act 1988 (Cth) and the Health Records and Information Privacy Act 2002 (NSW), Twenty10 staff or volunteers will not record or disclose to anyone else including team members, the HIV/AIDS status of a service user, volunteer or a staff member.

2.4. Privacy for interviews and personal discussions

To ensure privacy for clients or staff when discussing sensitive or personal matters, the organisation will:

- provide private consultation rooms where confidential information can be discussed;
- ensure that no one else is in the room when confidential information is being discussed;
- ensure that sensitive phone calls are taken in offices or other private spaces only; and
- ensure that records of any sensitive oral communications are stored securely in a manner consistent with the maintenance of that confidentiality/privacy;

2.5. Participants in research projects

People being invited to participate in a research project must be:

- given a choice about whether to participate;
- given the right to withdraw at any time;
- informed about the purpose of the research project, the information to be collected, and how the information they provide will be used.
- given copies of any subsequent publications.

The collection of personal information will be limited to that which is required for the conduct of the project. Individual participants will not be identified.

Organisational participants in research projects will generally be identified in Twenty10's research, unless the nature of a particular project requires anonymity, or an organisation specifically requests it.

2.6 Confidentiality and the Board

Confidentiality Is a Fiduciary Responsibility of Board Members, meaning they must act honestly and put the best interests of the organisation ahead of their own interests. Board Members shouldn't disclose information that they've received as part of their position on the board. Further they must not improperly use the information to gain advantage for themselves or someone else, or cause detriment to the organisation.

The obligation to maintain confidentiality continues to apply even after a person has left the Board. Board members must return all confidential information and documents to the Public Officer (Co-Executive Directors) within 14 days of their resignation from the Board.

Confidential documents may include, but are not limited to: Agendas, Minutes, and Board Papers for Board or Sub-Committee meetings, Financial Reports, Board Discussion papers, recruitment and personnel files or documents, AGM or EGM papers, records of grievances or complaints, reports and statistics around service use, printed copies of emails, electronic files of any of the aforementioned etc.

Should a Board Member breach this policy, unknowingly or not, the Board may decide to expel them from the Board depending on the circumstances of the breach.

For more information see [P02.1 Governance, section 2.4.3 Confidentiality]

3. Frequently Asked Questions

Q: What do we need to tell clients about privacy and confidentiality during intake?

A: We must tell clients that it is their right that their confidential information:

- stays private;
- is collected for a reason;
- can be changed or deleted at their request;

Q: Can a person withdraw their consent?

A: Yes. A person may withdraw their consent to data collection at any time.

Q: Does someone have to agree to have their information collected to access services?

A: No. Giving consent to having information collected is not a prerequisite for accessing services.

4. Where to Go For Help

For more information on this Policy, speak with the Co-Executive Directors.

5. Definitions

Board members: Members of the Twenty10 incorporating GLCS NSW Board.

Confidential information: Personal or organisational information that needs to remain private. This includes, but is not limited to personal contact details, proprietary information, and information that could be linked to a client. Often this information has been provided on the basis that it is not disclosed to other people or organisations.

Partner organisation: An organisation that works with Twenty10. This includes organisations that co-manage clients with us.

Proprietary information: Information about the organisation that needs to remain private. This includes, but is not limited to organisation planning, financial transactions, competitive tenders, and other activities identified by the Board.

Privileged Communications: Communications between a person or organisation from their legal advisor on a confidential basis that relate to either legal advice or litigation.

6. Publication and distribution of information

The Office and Administration Manager will upload this document to Google Drive.

DOCUMENTATION

Documents related to this policy	
Related policies	[P1.5 Ethical framework] [P02.5 Conflicts of interest] [P05.6 Professional ethics and conduct] [P09.7 Client records] [P09.25 Child protection and safety] [P11.3 External communication] [P11.6 Access to confidential information]
Forms, record keeping or other organisational documents	[Code of Ethics and Conduct Agreement]

Roles referred to this policy

Co-Executive Directors Office and Administration Manager Communications and Project Support Officer

Policy context: This policy relates to	
Standards or other external requirements	NSW Specialist Homelessness Services - Standard 1 DSS Data Exchange terms of service CIMS terms of service
Legislation or other requirements	Federal Privacy Act, 1988 (Cth) Australian Privacy Principles Freedom of Information Act 1982 Social Security (Administration) Act Privacy and Personal Information Protection Act 1998 No 133 (NSW); Public Health Act 2010 (NSW) Health Records and Information Privacy Act 2002 No 71 (NSW) The Children and Young Persons (Care and Protection) Act 1998 (NSW); and The Housing Act 2001 (NSW).
Contractual obligations	Secure record keeping and data collection (e.g. confidential records to be kept in locked file in a locked room (FACS, Reconnect) Names and identifiable information not kept in call or chat logs (Qlife).

Reviewing and approving this policy		
Frequency	**Person responsible**	**Approval**
Annually	Co-Executive Directors	Board

Policy review and version tracking			
Version / Review	**Date Approved**	**Approved by**	**Next Review Due**
1.0	05/02/2018	Stephen Garofano, Atari Metcalf	01/02/2019
2.0	19/11/2019	Elizabeth Duck-Chong	01/11/2020

3			