3.03 Privacy & Confidentiality of Consumers

Original Ratification Date	14/11/2018
Persons affected by Policy	All management and Team Members
Who is Responsible	Governance Body
Reviewer	Executive Officer
Terms	The Service – Community Links Wellbeing Team Member – Employees & Volunteers unless otherwise stated Project – Individual projects auspiced/ run by Community Links Wellbeing Governance Body – The governing body of Community Links Wellbeing

POLICY STATEMENT

The organisation will ensure it abides by the Australian Privacy Principles when dealing with information provided to us by the consumer.

PROCEDURES

Notes:

Information regarding Retention of Records, Electronic Information Management, Use of Technology & Privacy is detailed in Section 5 Operational Management – Information Management, Use of Technology & Privacy

Information regarding the organisations commitment to privacy and the Australian Privacy Principles is detailed in Section 1 Governance– Privacy & Access to Information

Information regarding consent, collection and provision of information is contained within 3.05 Decision Making, Intake and Service Provision

This and the policies mentioned above apply to:

- all team members, past and present;
- any person who obtains information about consumers through the activities of the organisation;

The privacy and confidentiality of consumers applies:

- in the workplace;
- at home;
- when talking with other team members;

- when dealing with team members of other agencies or institutions;
- in social environments;
- when talking with other consumers.
- Volunteers and students

Abuse of, or carelessness with, confidential information can not only compromise the dignity and independence of an individual but can in some cases pose a direct threat to their health and safety. Protecting the privacy of consumers and ensuring stored information is properly used at all times is therefore of paramount importance to the organisation. Confidential information can occur in verbal, written, photographic, audio or computer record form. Information collection should be as non-obtrusive and objective as possible, yet relevant and up-to-date.

It is a breach of privacy/confidentiality if a person's private information is disclosed by another person without the legal authority to do so. Privacy/confidentiality is everybody's responsibility. Should a team member breach another person's privacy/confidentiality without the legal authority to do so, they may be held liable for prosecution under the Privacy and Personal Information Protection Act 1988.

Privacy & Confidentiality is between the consumer and the organisation NOT individual team members (unless directed by legislation). Discussion of service provision issues is a necessary part of team member supervision and is not a breach of privacy. Discussion of issues outside supervision may be acceptable in incidents of peer support as long as the identity of the consumer and other information that may indicate the identity of a consumer is not disclosed.

All team members will sign a Code of Conduct and Confidentiality Agreement. Team members/contractors who, in the course of their work, have access to records, files, or data belonging to or about others including team members shall take precautions to avoid invading the privacy of individuals without their knowledge. These people must not divulge or disclose such information to others, unless required by the service policy or State or Commonwealth law, and if required to disclose information must comply with the relevant guidelines in place relating to disclosure.

Discussing consumers with other's (excluding a supervisor), is strictly prohibited.

Information sharing with other organisations must only occur with the consumers permission detailed in an Authority to Exchange Information. (excluding information Under Section 16 of the Child Protection Act).

If an extreme situation arises where a breach of privacy/confidentiality may be required, discussion between the Team Manager regarding the extenuating circumstances will occur before making a decision to breach privacy/confidentiality. A report on the circumstances will be recorded on the file of the person concerned, or in the case where there is no file, in a confidential folder and placed in a secure location.

3.03-1 Privacy Statement

The organisation's Plain English Privacy Statement will be published on the website and be provided to consumers at intake.

Should this section be changed, 3.03a Privacy Statement should also be amended

Privacy Statement

At Community Links Wellbeing we **promise** you:

- **We follow the Australian Privacy Principles** to make sure we keep your information safe. You can have a look at the principles at https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/national-privacy-principles
- **We will only collect the information we need** to provide you with a safe high quality service;
- **We will tell you why we need the information;**
- **We will only discuss your personal information** with Community Links Wellbeing team members to provide the best service to you; you provide consent to refer and exchange details with external agencies/ or if an emergency.
- **Your records detail what happens during service** and enables our team members to provide you with a service which is relevant, informed and focussed on you.
- **We will not give anyone access to your information** without your permission **UNLESS** you are in danger (for example if there is an accident we will supply information to the ambulance officers) or we are required to under law;
- **We will give you every opportunity to ensure the information we hold about you is correct**. Sometimes we will go over the information we hold, with you, just to make sure. If you think we may have outdated information, please call us;
- **In our office we keep your information safe**; our computers are all password protected, our filing cabinets are kept locked and only used by team members who have had police checks and have signed our Code of Behaviour and Confidentiality Agreements. If we have to give access to our systems, to a third party, we make sure our contract with that agency protects your information (for example if we need to get the computer fixed our contract with the computer company says they can't access or use your information);
- **If for some reason we think your information may have been lost or stolen,** we will let you know straight away and talk to you regarding options you may want to consider to safe guard your identity;
- **We will never give or sell** your information to anyone (e.g. marketing companies etc);
- **We are required to collect** summary information / statistics for the purpose of meeting our funding body's reporting requirements.
- **We will let you see any information** that we have collected about you (just call us to arrange an appointment if you want to see your records);
- **We want to hear what you think** about our service – it helps us improve – if ever you would like to give feedback anonymously that is also fine;

If you want **more information** just contact us.

3.03-2 Australian Privacy Principles

Development of this policy and procedure has been guided by relevant Australian Privacy Principles, for further information go to https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles as detailed below:

- Australian Privacy Principle 1—open and transparent management of personal information
- Australian Privacy Principle 2—anonymity and pseudonymity
- Australian Privacy Principle 3—collection of solicited personal information
- Australian Privacy Principle 4—dealing with unsolicited personal information
- Australian Privacy Principle 5—notification of the collection of personal information
- Australian Privacy Principle 6—use or disclosure of personal information
- Australian Privacy Principle 7—direct marketing
- Australian Privacy Principle 8—cross-border disclosure of personal information
- Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers
- Australian Privacy Principle 10—quality of personal information
- Australian Privacy Principle 11—security of personal information
- Australian Privacy Principle 12—access to personal information
- Australian Privacy Principle 13—correction of personal information

The Service is committed to collecting, keeping and disposing of records in ways that protect privacy and ensure confidentiality is maintained. This policy will operate in conjunction with project specific procedures.

Specifically, the service will ensure each project:

- collects and keeps information about consumers only when it is relevant and necessary to the provision of the service
- ensure data about each consumer is up to date, accurate and secure, whether stored in hard copy or electronically, in accordance with privacy legislation
- take account of any relevant cultural or religious sensitivities of people using services in the way information about them is collected, stored and used
- store consumers records for the required length of time
- transfer or dispose records of consumers correctly

3.03-3 Data Breach *Note: Should information in procedure change the Emergency & Critical Incident Action Plan must also be amended*

Privacy Amendment (Notifiable Data Breaches) Bill 2016 requires all businesses already subject to the Privacy Act with an annual turnover more than $3 million to notify the Office of the Australian Information Commissioner (OAIC) and the affected individuals of an eligible data breach as soon as practicable after the organisation is aware that there are reasonable grounds to believe that there has been an eligible data breach.

Data breaches occur in a number of ways. Some examples include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased
- databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the agency or organisation
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins
- an agency or organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving an agency or organisation into improperly releasing the personal information of another person.

Dealing with a suspected data breach will form part of the Emergency & Critical Incident Action Plan.

The Data Breach Roles & Responsibilities flowchart details team member's responsibility if they suspect a data breach may have occurred.

The Executive Officer will ensure the Data Breach Investigation Flowchart below is followed should they be notified of a data breach or suspected breach.

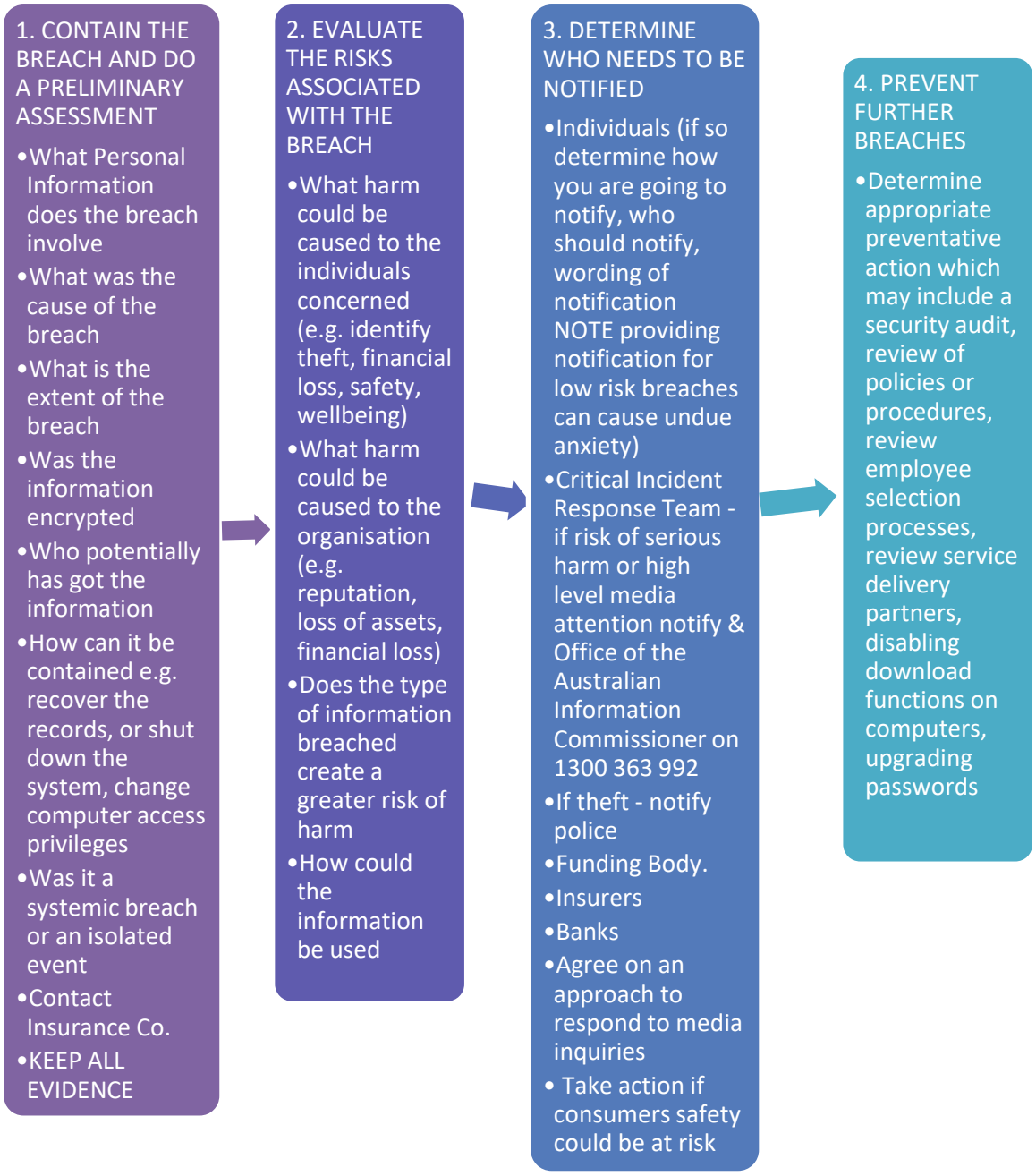
Notifying individuals when a data breach involves their personal information supports good privacy practice, for the following reasons:

- *Notification as a reasonable security safeguard* – As part of the obligation to keep personal information secure, notification may, in some circumstances, be a reasonable step in the protection of personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure (as required by APP 11).
- *Notification as openness about privacy practices* – Being open and transparent with individuals about how personal information may be handled is recognised as a fundamental privacy principle. Part of being open about the handling of personal information may include telling individuals when something goes wrong and explaining what has been done to try to avoid or remedy any actual or potential harm.

- *Notification as restoring control over personal information* – Where personal information has been compromised, notification can be essential in helping individuals to regain control of that information. For example, where an individual's identity details have been stolen, once notified, the individual can take steps to regain control of their identity information by changing passwords or account numbers, or requesting the reissue of identifiers.
- *Notification as a means of rebuilding public trust* – Notification can be a way of demonstrating to the public that an agency or organisation takes the security of personal information seriously, and is working to protect affected individuals from the harms that could result from a data breach. Customers may be reassured to

know that an agency or organisation's data breach response plan includes notifying them, the OAIC, and relevant third parties.

- The OAIC strongly encourages notification in appropriate circumstances as part of good privacy practice, and in the interest of maintaining a community in which privacy is valued and respected.



3.03-4 Our consumer Accessing their Records

Consumers have the right to read any personal information kept about them by the service. Requests from the person to access files should be in writing and referred to the Team Manager who should ensure that assistance is provided for the person to

access information on his/her file within two weeks. A team member should be made available to explain any terminology to the person.

When a consumer requests information from the service, they are advised of the privacy and release of information procedures within the organisation including that information is kept confidential on a secure computer protected by passwords that only appropriate team members have access to.

The only people authorised to read a person's file are the person themselves, the person's proven representative/advocate and/or the person's legal guardian. Advocates must have the consumers permission in writing, where this can be given.

Before authorising access to a legal guardian, a thorough examination should be conducted to confirm that no active court orders, Apprehended Violence Orders (AVOs), or similar legal directives are currently in effect.Access to some information may breach confidentiality of team members or another consumersand this information may be withheld.

3.03-5 Team Member's/Contractors Accessing Records of Consumers

Only team members with a need (i.e. those involved with the care of consumers, supervision of team members) will have access to personal information related to consumers or team members.

Records of consumers are available to the team member and their direct supervisor for direct supervision only. Other team members at the service will only read a consumers file when it is required to carry out work with that consumer.

Any sub-contractors which the service utilises will be required to provide confirmation that their policies and procedures comply with the appropriate privacy laws.

3.03-6 Files of Consumers

Files will only contain information necessary to provide a quality service to consumers.

- Notes documenting interactions with the individual will be maintained, and may include:Intake;
- Assessment;
- NDIS Plans and Service Agreements
- Development of individual /development program plan;
- Review of individual development/program plan;
- Progress reports and other relevant information;
- Change in circumstances;
- Complaints;
- Reports / information from other agencies; or
- Requests for any change in service
- Closure reports
- And group reports.

All entries in the records will indicate the time and date the entry was made, and

enable the reader to identify the name and designation of the writer.

All note entries in the records will be written in ink so that they will not fade or be erased.

Files removed from the office should be placed inside locked bags allocated to each project.

If a person transfers between projects within the service, their case file will be closed in one project and reopened in the new project. An authority to transfer relevant information should be sought from the consumer

3.03-7 Release of Information under Duty of Care

Information about a consumer will not be shared with another agency without the permission of the consumer using an Authority to Exchange Information or his/her legal guardian or advocate unless the organisation has a legal obligation to do so, personal information regarding a consumer or team members may be disclosed if:

- Informed consent is obtained from the person and this consent specifies the precise information and purpose for the disclosure;
- There is a risk of serious harm to a child's life, health or safety;
- There is a serious and imminent threat to an adult's life, health or safety;
- There is a serious threat to public health or public safety; or
- There is a legal obligation under:
    - the Crimes Act 1900 (NSW),
    - the Crimes Act 1914,
    - the Children's Care and Protection Act 1998 or
    - the Coroners Act 1980 (NSW) to notify police about serious criminal offences, or the coroner's office regarding investigations involving the death of a person.

Confidentially is between the consumer and agency (not particular team member or projects). Team members will inform the person that they have to report any information that may impact upon the service provided to the office.

In cases of emergencies the 'first contact' or nominated person/advocate on the CLW's database's will be contacted to make immediate decisions about wellbeing. Where a duty of care matter arises after reasonable discussions have concluded that a decision must be made 'first contact' will provide permission.

In all circumstances only information relevant to the purpose will be given (e.g. In the case of a medical emergency only that information which is relevant to the emergency and is needed by Emergency Services to provide appropriate care will be provided)

A summary of actions must be maintained and stored on Person's file identifying at a minimum

- Date
- Type / reason for emergency
- Actions taken prior to passing on information regarding a consumer

- Level of information passed on
- To whom the information was passed onto.
- Date our consumer informed of actions and person's response
- Reason for undertaking action

3.03-8 Freedom of Information

Documents disclosing information about someone's personal affairs to another are exempt from Freedom of Information Act (FOI legislation). This exemption is to protect the privacy rights of individuals and it will prevent someone from obtaining details regarding the personal affairs of another (whether that person is dead or alive). 'Personal affairs' includes, but is not limited to Information pertaining to the:

- address,
- age,
- medical history,
- family situation,
- employment,
- sexual preference,
- social security status,
- financial situation
- criminal record of an individual.

3.03-9 Group Processes and Privacy/Confidentiality

At the start of the group the leaders are required to advise participants of the service's mandatory reporting obligations in respect of child protection, self-harm and harm to others.

At the first session of a group program, group leaders need to inform group members of the issues and guidelines around privacy/confidentiality. See Project Specific Working with Groups Procedures linked to 3.05 Decision Making, Intake & Service Provision

3.03-10 Participants in Research Projects

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

- given a choice about participating or not
- given the right to withdraw at any time
- informed about the purpose of the research project, the information to be collected, and how 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. The individual participants will not be identified

The anonymity of consumers and team members will be preserved for purposes of research, case presentations or conference papers unless specific permission has been granted by the person.

3.03-11 Privacy for Interviews and Private Discussions

Team members should endeavour to protect the privacy of others by finding private space to meet and by making sensitive telephone calls away from the hearing distance of others. If private space unavailable; team members to ensure environment is safe to discuss. All team members are bind by Privacy and Personal Information Protection Act 1998.

3.03-12 HIV AIDS Information

A person's HIV AIDS status has special legal protection in the NSW *Public Health Act*. Team's must not record in any document, or disclose to anyone else **including team members**, a person's HIV AIDS information, unless that information is strictly necessary in order to provide care, treatment or counselling to that person. (For example, you must not record or disclose HIV AIDS information solely to protect other people from infection e.g. in accommodation or recreation programs).

3.03-13 Storage and use of Identifiable Data

Information collected about individual consumers is stored in the following ways:

- In the team members locked filing cabinet which can be checked by the Team Manager from time to time for quality control, and by other teams in the case of an emergency i.e. someone's safety is at risk or the team member has suddenly fallen ill/left in which case another team member will be appointed
- Electronically with security access only (of which the same processes as the previous point will be applied)

Consumers or team members will be informed of the service's responsibilities in relation to the protection of personal information through Consent to Service Agreements.

See Section 5 *Information Management, Use of Technology & Privacy for more information.*

3.03-14 Loss or Theft of Files

Loss or theft of a file or record containing personal information must be investigated and reported to the relevant manager immediately and the Critical Data Breach Procedures within the Services Critical Incident Action Plan will be followed.

3.03-15 Legal Requirements of Electronic Correspondence/Information

For legal purposes e-mail has the same standing in court as paper documents. The service can be involved in litigation and relevant records relating to use and activities in relation to e-mail, internet and intranet are "discoverable" by way of court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of team members, our consumers, or third parties as well as any relating to research, or other communications even if communicated in confidence. For more information regarding:

- Electronic information management
- Classification of electronic correspondence,

- Email retention & archiving
- Storage of electronic communication/information
- Ownership of email addresses
- Internet usage
- Monitoring internet usage
- Internet/electronic communication conduct requirements
- Internet relay chats

Please see section 5 of the Policy & Procedure Manual

DOCUMENTATION

Documents linked to this policy	
Forms, record keeping or other organisational documents	3.03a Privacy Statement 3.03b Authority to Exchange Information 3.03c Suspected Data Breach Flowchart (updated) 3.03d Data Breach Investigation 3.03e Voluntary Group Confidentiality Agreement

Review and version tracking		**Date Original Approved:**
BNG Version	**Date This Review Approved:**	**Next Review Due**
1	Executive Officer 12/11/2020	12/11/2021
2	Executive Officer 31.08.2022	31.08.2023
3	Executive Officer 01.02.2023	01.02.2024
4	Executive Officer 25.11.2025	25.11.2026

Policy context: This policy relates to	
Legislation or other requirements	Human Rights and Equal Opportunity Commission Act (Commonwealth) 1986 UN Convention on the Rights of the Child Anti-Discrimination Act (NSW) 1977 Sex Discrimination Act (Commonwealth) 1984 Children and Young Persons (Care and Protection) Act 1998 (NSW) Commission for Children and Young People Act (NSW 1997) Child Protection (Working with Children) Act (NSW), 2012. Child Protection (Working with Children) Regulation (NSW), 2013. Freedom of Information Act (Commonwealth) 1982, (State) 1989 Community Services (Complaints, Reviews and Monitoring) Act 1993 (NSW) Privacy and Personal Information Protection Act 1998 (NSW) The Australian Privacy Principles 2014 Guardianship Act (1987) NSW Powers of Attorney Act (2003) NSW Carer's (Recognition) Act 2010 Racial Discrimination Act 1975 (Commonwealth) Disability Discrimination Act 1992 (Commonwealth) Age Discrimination Act 2004 Disability Inclusion Act 2014 No 41 (NSW) Disability Services Act 1986 (Commonwealth) Children and Young Persons (Care and Protection) Act 1998 Crimes Act 1914 (Commonwealth) Criminal Code 1995 (Commonwealth) Health Records and Information Privacy Act 2002 (NSW). Funding Agreements NSW Family Services Principle Case Management Society of Australia National Standards NDIS Act (2013) NDIS Practice Standards Australian Charter of Healthcare Rights Australian Open Disclosure Framework Case management Society of Australia and New Zealand Standards NSW Modern Slavery Act 2018 NSQDMHS and NSQMHSCMO Practice Standards
Definitions	
Confidentiality	Keeping information that is private and personal obtained through the course of employment or disclosed by the Our consumer, other team, community partners or the Management Committee private.
Personal Information	Personal information includes all information that identifies or describes an individual. This includes information that is or is not stored in a database.
Statutory Requirement	This is an enactment made by a legislature and expressed in a formal document which must be abided by.
Mandatory Reporting	This is the protocol whereby, primarily those who work with children are required by law to report to the relevant child welfare authorities anything of a prescribed nature (usually evidence of potential child abuse & neglect) that comes to their attention in the course of their duties.