03CLI-159

Privacy and Confidentiality

Document Number:	03CLI-159	Document Owner:	Service Delivery
Version Number:	001	Approved By:	EGM, Service Management and Development
Date of Issue:	23/03/2018	Signature	On File
Date to be Reviewed	23/03/2021	Date Signed	On File

Table of Contents

Purpose

The purpose of this policy is to establish OAK Possability's standards of privacy, dignity and confidentiality with respect to prospective, current and past users of our services as well staff and stakeholders. OAK Possability respects the privacy of all people including employees, service users, business partners, members, volunteers, donors and online users, and is committed to safeguarding the personal information that is provided to us. The purpose of this Policy is to:

- Clearly communicate the personal information handling practices of OAK Possability,
- Enhance the transparency of OAK Possability operations,
- Give individuals a better and more complete understanding of the sort of personal information that OAK Possability holds, and the way we handle that information.

OAK Possability is committed to protecting client privacy and confidentiality of personal information that the organisation collects, in accordance with current legislation.

Policy Principles

OAK Possability acknowledges and respects the privacy and confidentiality of individuals. Confidentiality relates to the treatment of information that has been disclosed during the course of a professional relationship. OAK Possability employees have an obligation to respect client privacy and confidentiality at all times in their interaction with other employees of OAK Possability and persons external to OAK Possability and refrain from disclosing information that is given in confidence. Staff should always use their discretion and judgement when discussing work issues, ensuring that private information is not shared outside of the service unless required for service purposes and with appropriate written authorisation. In support of this principle, all employees sign a legally binding (in perpetuity) *HUR-F021 Collection of Employee Information* at commencement of employment with OAK Possability.

All personal information will be protected and managed according to the relevant legislation. The following legislation guides this policy:

- Privacy Act 1988,
- Australian Privacy Principles (January 2014),
- Privacy Amendment (February 2018),

Under the Australian Privacy Principles[1], OAK Possability is required to advise persons whose information is being held, how the information is being collected, what is being collected, why it is being collected, information about the complaints process and whether or not the information is being disclosed to overseas recipients. The Privacy Amendment[2] is concerned with OAK Possability's reporting responsibilities to individual's whose information is being held and to the Office of the Australian Information Commission, in regards to data breaches.

[1] See https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles
[2] See https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

Procedure/Process

The following procedures are to be implemented to ensure that OAK Possability meets its legislative and policy obligations. OAK Possability policy objectives are to ensure that our clients have the same level of privacy, dignity and confidentiality as is expected by the rest of the community.

1.1 OAK Possability Employees will ensure they:

- Only collect information about the client that is directly relevant for service delivery and OAK Possability's duty of care responsibilities,
- Gain written consent of the client, family, carer or advocate prior to **obtaining or releasing** information from any other person, agency or service,
- Ensure that personal information is stored securely and confidentially and is not left for unauthorised staff, visitors or the general public to view,
- Ensure that only those staff who 'need to know' have access to relevant client information,
- Ensure that personal information about the client is only held by OAK Possability as long as it remains relevant to the delivery of services, OAK Possability's duty of care, and legal obligations,
- Promptly investigate, remedy and document any client complaint regarding privacy or confidentiality,
- Implement the *01QUA-020 Clear Desk and Clear Screen Policy*.

1.2 OAK Possability will:

- Maintain IT security protocols to ensure that personal information is kept safe and secure,
- Ensure that all personal information held (clients and staff) is accurate, up to date, complete and relevant, through a process of regular reviews for the accuracy of content and disposed of appropriately when not relevant or needed (per OAK Possability policies),
- Gain agreement from all staff/contractors/volunteers to uphold OAK Possability's policies and processes regarding the safekeeping of client personal information through the induction process
- Advise the client, family, carer or advocate of the nature of the personal information that is held and their right to view and request any changes to their own information,
- Ensure that consent for any sharing of information (outbound or inbound) is gained from clients,
- Advise clients, family, carer or advocate of their right to complain and the complaints process – including their right to use a pseudonym (assumed name) when making a complaint,
- Advise clients, family, carer or advocate of their right to view this policy
- When sending marketing materials to clients – ensure that they are provided with an 'opt out' choice and ensure that if they do select to opt out that this is enacted,
- Provide the client, family, carer or advocate with a copy of either of the following booklets: Working together: How we work with you (Plain English version (December 2016); or Working Together: Our policies and practices (June 2016).
- Conduct regular privacy audits to ensure that OAK Possability is being proactive in monitoring clients' privacy.

2. Employee/Volunteer Information

OAK Possability collects information on employees, prospective employees, contractors and volunteers.

Information collected may include some or all of the following:

- Contact details (name, address, telephone numbers, email etc.),
- Personal details including personal details of emergency contact person(s),
- Date of birth,
- Country of birth, citizenship, residency and/or visa details,
- Details of current/previous employment or volunteer involvement,
- Skills and experience,
- Languages spoken and written,
- Qualifications, drivers licence details,
- Bank details (if OAK Possability is to receive payment or make payment for services received).
- Australian Business Number (ABN),
- Information and opinions from referees for prospective employees and candidates for volunteer work,
- Police Checks,
- Pre-employment health check.

Employee information is collected to process an application for employment, volunteering or to become a member of OAK Possability; facilitate a placement; assist with services; provide feedback; assist in improving programs and services; to process donations and provide receipts; to receive and/or pay for services; to establish and manage partnerships; to provide information about services; facilitate further involvement in the organization and to meet legislative requirements.

3. Client Information

Client information is collected to provide services that meet client needs; monitoring/evaluating programs; to produce annual reports; to meet with government funding requirements; and to comply with legal requirements. Sometimes client information is used for to improve public awareness or for educational purposes through contact with the media, speeches, event management, surveys and publication preparation. The personal information on public awareness and education files is not disclosed to other organisations or anyone else without consent unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those organisations or individuals, or the disclosure is otherwise required or authorised by law.

Client information is collected through service applications, assessments and online/phone enquiries. We collect:

- Contact details (name, address, email etc.),
- Personal details including: date of birth, gender, income,
- Information on personal issues and experiences, relationships,
- Family background, supports clients may have in the community,
- Areas of interest,
- Health information and/or medical history,
- Bank account and financial details.

Where possible, personal and sensitive information is collected directly from the client, through, for example, telephone and in-person interviews, appointments, forms and questionnaires. In some situations we may also obtain personal information about a client from a third party source but will take all reasonable steps to contact

the client and ensure that they are aware of the purposes for which we are collecting their personal information and the organisations to which we may disclose that information, and gain written consent. For example, information may be collected about the client from a health care professional, such as a GP.

3.1 Client Consent

At first contact, OAK Possability clients will be asked to read and sign a *CLI-002 Authorisation to Receive and Release Information*. This will permit OAK Possability to receive information from, and release information to, other relevant support services, agencies, bodies and/or health professionals, about the client. Clients are also asked to authorise the use of photographic images for official business, including: websites, newsletters, newspapers and promotional material. Where consent is given it cannot be rescinded for the life of the published material.

OAK Possability will not use health information beyond the client consent provided, unless further consent is first obtained or it is in accordance with one of the exceptions under the Privacy Act or in compliance with another law. If OAK Possability uses client health information for research or statistical purposes, it will first be de-identified, if practicable to do so.

Consent is reviewed every twelve (12) months, however, at any time clients or staff are able to ask for this to be reviewed.

4. Member Information

Members of the organization may have the following information collected:

- Contact details (name, address, telephone numbers, email etc.),
- Date of birth,
- Credit card details and expiration date,
- Expiration date of credit card,
- Areas of interest.

This information is used to provide services; provide communication updates; process donations and provide receipts; facilitate fundraising and marketing activities; provide organizational information; receive invitations about upcoming events/activities; and to recognise member support.

5. Website Information

The OAK Possability website may, from time to time, contain links to other websites. OAK Possability stresses that when an online user accesses a website that is not the OAK Possability website, it may have a different privacy policy. To verify how that website collects and uses information, the user should check that particular website's policy.

6. Donor Information

Information on donors is collected through communication (email, online, phone) and flyers. The following information may be collected:

- Contact details (name, address, telephone numbers, email etc.),
- Personal details including: date of birth, gender, income,
- Areas of interest,
- Donation history,
- Credit card numbers (and expiration date) or bank account details.

This information is used to provide services; process donations and provide receipts; facilitate fundraising and marketing activities; ensure transparency in relation to donated funds; and to comply with legal obligations.

7. Online User Information

Online data that is collected includes:

- Contact details (name, address, telephone numbers, email etc.),
- Non-personal information e.g. visitor navigation and statistics,
- Server address, browser type, date and time of visit,
- Personal information.

OAK Possability uses this information to: analyse website usage and make improvements to the website. Personal information is not matched to non-personal information collected.

8. Mailings Lists

OAK Possability maintains contacts lists which include contact information about individuals who may have an interest in disability services. We use these contacts lists to distribute information about our activities and publications. We do not share these lists outside of OAK Possability.

Personal information for contacts lists are sourced directly from individuals, for example, where they have asked to be added to a contact list, or sometimes from a third party or from a publicly available source such as a website or telephone directory. Information from a third party is only collected in this way if the individual would reasonably expect us to, or has given their consent. For instance, we might collect this information if we thought that the individual (or the organisation they work for) would like to receive information about services we are carrying out, or that they might be likely to consider information about disability care useful in the work they do. We would only contact this individual in their work capacity.

We only use personal information in contacts lists for the purpose of managing stakeholder relations. We do not give personal information about an individual to other organisations or anyone else without consent unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those organisations or individuals, or the disclosure is otherwise required or authorised by law.

We maintain and update personal information in our contacts lists when we are advised by individuals that their personal information has changed. We also regularly audit contacts lists to check the currency of the contact information. When receiving marketing materials, recipients are free to 'opt out' of receiving such materials,

should they wish to do so. Upon receiving a request to 'opt out' the individual is removed from the mailing list.

9. Security of Personal and Sensitive Information

OAK Possability takes all reasonable steps to protect the personal and sensitive information we hold, against misuse, interference, loss, unauthorised access, modification and disclosure. These steps include password protection for accessing our electronic IT system, securing paper files in locked cabinets and physical access restrictions. Only authorized personnel are permitted to access these details.

Routine access to contacts lists is limited to the database operators who have responsibility for maintaining the contacts lists. Other staff members have access to the personal information in contacts lists on a need to know basis. Access to public awareness and education files is granted to only senior management, marketing and human resources staff.

When the personal information is no longer required by either OAK Possability or under an Australian Law or court/tribunal order, it is destroyed in a secure manner, de-identified or deleted according to *01QUA-032 Document Management and Control.*

10. Sharing of Information

OAK Possability cannot use or disclose information for a purpose other than what it was collected for, unless:

- The individual consents to the use or disclosure or,
- The individual would reasonably expect OAK Possability to use or disclose the information for the secondary purpose and related to the primary purpose or,
- The use or disclosure is required under an Australian Law or a court/tribunal order or,
- A permitted general or health situation exists in relation to the use or disclose of the information or
- The use or disclosure is for government related identifiers or,
- It will prevent or lessen a serious threat to somebody's life, health or safety or to public health or safety or,
- It is reasonably necessary for us to take appropriate action in relation to suspected unlawful activity, or misconduct of a serious nature that relates to our functions or activities or,
- It is reasonably necessary to assist in locating a missing person or,
- It is reasonably necessary for a confidential dispute resolution process or,
- It is necessary to provide a health service or,
- It is necessary for research or the compilation or analysis of statistics relevant to public health/public safety,
- If the personal information is being used for the purpose of direct marketing.

10.1 External Agencies

From time to time, OAK Possability is mandated to share or provide information with approved organizations. For OAK Possability clients, these may include:

- Government departments/agencies who provide funding for OAK Possability services,

- Contractors who manage some of the services we offer, such as distribution centres who may send information to clients on behalf of OAK Possability[3].
- Doctors and healthcare professionals, who assist us to deliver our services,
- Our professional advisors, including our accountants, auditors and lawyers.

Information pertaining to staff, volunteers, and candidates for employment may be shared with:

- Government departments/agencies who provide funding for OAK Possability services,
- Other regulatory bodies, such as WorkSafe,
- Referees and former employers of Oak Possability employees and volunteers, and candidates for OAK Possability employee and volunteer positions,
- Our professional advisors, including our accountants, auditors and lawyers.

Information pertaining to clients, staff or volunteers may be shared with overseas entities from time to time, for example, for a joint research project initiative. At such times the following rules will apply:

- Shared information will be cumulative and de-identified,
- The recipient will be subject to a law similar to the Australian Privacy Principles in terms of protection of the information or an agreement to the same conditions of protection will be sought from the recipient in a contract, prior to the sharing of information,
- The aim of the sharing will be for the purpose of the development and/or improvement of OAK Possability services, and
- Consent for the sharing of such de-identified personal information will be gained through the completion of the *CLI-002 Authorisation to Receive and Release Information*.

10.2 Client Requests

Requests by clients to access or change their own personal information will be granted, unless there is a sound reason to refuse. The process will involve:

- Client request in writing and proof of identity to be received,
- Approval sought/gained from the OAK Possability Privacy Officer,
- Processing to be provided within 14 days of request (30 days if request is complicated or a large volume of information is involved),
- Summary of most recent information held to be created/shared and/or provision of access to inspect, take notes or print out personal information for the client,
- Update/complete information if client informs that it is inaccurate or out of date.

OAK Possability may charge clients a reasonable fee to reimburse for the cost incurred in accessing information, for example, for photocopying and delivery cost of information stored off site. For current fees, please contact the Privacy Officer.

[3] Steps are taken to ensure they comply with the Australian Privacy Principles (APPs) when they handle personal information and are authorised only to use personal information in order to provide the services or to perform the functions required by OAK Possability

Access will be denied if:

- 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 or would prejudice law enforcement activities or would prejudice an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of OAK Possability,
- Access discloses a 'commercially sensitive' decision making process or information.

If we deny access to information we will set our reasons for denying access. Where there is a dispute about a right of access to information or forms of access, this will be dealt with in accordance with the complaints procedure set out below.

10.3 Notifications

OAK Possability is mandated, under the Australian Privacy Principles, to notify individuals of the collection of personal information. For clients, primary notification occurs through the completion of the *CLI-002 Authorisation to Receive and Release Information*, where clients are advised of the collection and use of personal information and consent to a list of external organizations being either sources or recipients of their private information.

OAK Possability must also, under the Australian Privacy Principles, notify individuals if their personal information is to be collected from or shared with, entities other than those listed on the *CLI-002 Authorisation to Receive and Release Information* (and at this time, consent from the individual re-affirmed). The individual must be advised of the fact that the organization is collecting information, why the information is required, details of any court/tribunal order (if relevant), the purpose, the consequences if not collected, the process for seeking access to and correcting the information and information about the rights and processes concerning complaints. Therefore, when seeking or providing personal information, OAK Possability staff must check to see that we have consent for that action on file and if not, seek approval and a new *CLI-002 Authorisation to Receive and Release Information* to be completed with the updated information, as soon as possible.

11. Complaints

Persons with personal and sensitive information being held at OAK Possability have the right to make a complaint and have it investigated and dealt with under our complaints procedure. A privacy complaint relates to any concern that an individual may have regarding OAK Possability's privacy practices or the handling of an individual's personal and sensitive information. This could include matters such as how the information is collected or stored, used or disclosed or how it is provided.

The complaints process includes:

- Contacting the Privacy Officer to lodge the complaint,
- Complaints are logged on the database,
- Resolution of the complaint within 30 days through:
    - ***Request for further information***: The claimant needs to be prepared to as much information as possible, including details of any relevant dates and documentation. This will enable us to investigate the complaint and determine an appropriate solution. All details provided will be kept confidential,
    - Discuss options: We will discuss options for resolution with you and if you have suggestions about how the matter might be resolved you should raise these with our Privacy Officer,
    - ***Investigation:*** Where necessary, the complaint will be investigated. This may involve contacting others and/or engaging the services of an independent investigator to conduct the investigation,
    - ***Conduct of our employees***: If your complaint involves the conduct of our employees we will raise the matter with the employee concerned and seek their comment and input in the resolution of the complaint,
    - ***Request to alter information:***
        - ***Agreement to Correct Information***: If the complaint is found to be substantiated, the claimant will be informed, information will be updated and concerns addressed. Efforts will be made to prevent the problem from recurring,
        - ***Refusal to Correct Information:*** OAK Possability must provide a written notice that explains why it would be unreasonable to do so and advise their right to complain about the refusal. OAK Possability may refer the issue to an appropriate intermediary, for example, an appropriately qualified lawyer or an agreed third party, to act as a mediator,
    - ***Escalation:*** At the conclusion of the complaint, if the claimant is still not satisfied with the outcome, they are free to take the complaint to the Office of the Australian Information Commissioner[4], ***Documentation***: We will keep a record of the complaint and the outcome.

Under the Australian Privacy Principle, clients also have the right to anonymity when making a complaint. Complainants using pseudonyms (assumed names) must be accepted and the complaints process applied. The exception is where it is impracticable for OAK Possability to investigate the claim with individuals who have not identified themselves.

12. Unsolicited Personal Information

If OAK Possability receives personal information that was not purposively sought they must:

- Determine whether that information could have been reasonably collected through the individual's consent or access would have been mandated under Australian Law,
- If OAK Possability could not have obtained that information and it is not contained in a Commonwealth record, then it must:
    - Destroy the information or de-identify the information as soon as practicably able to do so.

[4] See *http://www.oaic.gov.au* for contact details.

13. Data Breaches

13.1 Notifiable Data Breaches (NDB) Scheme

The purpose of the NDB scheme is to protect people whose personal information has been released without their authority. Under the Privacy Amendment[5] Act, OAK Possability is mandated to notify the Privacy Commissioner of the Office of the Australian Information Commissioner (OAIC) and any affected individuals of any 'eligible' data breaches[6].

An eligible data breach occurs when the following three criteria are met:

1. There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds,
2. This is likely to result in serious harm to one or more individuals including:
    a. Physical Harm
    b. Financial/Economic Harm
    c. Emotional Harm (e.g. embarrassment or humiliation)
    d. Psychological Harm (e.g. marginalisation or bullying)
    e. Reputational Harm
3. The entity has not been able to prevent the likely risk of serious harm with remedial action.

OAK Possability is required to assess any suspicion of an eligible data breach and take all reasonable steps to ensure that the assessment is completed within 30 days. Reporting to the OAIC is via a Notifiable Data Breach Statement available on the OAIC website.

13.2 Notifying Affected Individuals

When there is a data breach OAK Possability will notify the individuals whose personal information has been accessed/compromised. This will involve utilizing one of three options:

- **Option 1**: Notify all individuals of the breach, allowing them to consider whether they need to take any action in response, or,
- **Option 2:** Notify only the individuals who are at risk of serious harm from the eligible data breach (avoids notification fatigue among members of the public and reduces administrative costs), and/or,
- **Option 3**: Publish notification on the website and take steps to publicise the contents of the statement (only if options 1 and 2 not practicable).

In option 1 and 2 individuals will be notified by the usual means of communicating with that individual (phone, SMS, mail, social media post, in-person conversation etc). The notification must include:

- OAK Possability name and contact details,
- A description of the eligible data breach,
- The kind/s of information concerned,
- Recommendations about the steps that people should take in response to the breach.

[5] Notifiable Data Breaches (Feb 2018), Retrieved 12 Feb, 2018 from https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

[6] Effective February 22, 2018.

In Option 3, reasonable steps when publicising an online notice might include ensuring the webpage which houses the notice can be located and indexed by search engines, announcing on social media channels and/or taking out a print or online advertisement in a publication which it is reasonably considered will reach the individuals.

13.3 Penalties

Where previously reporting was voluntary, the ratification of the Privacy Amendment now requires organizations like OAK Possability to report, conferring harsh penalties for failure to comply. A failure to notify constitutes a serious interference with privacy under the Privacy Act may result in a fine of up to AU$360,000 for individuals or AU$1.8 million (about US$1.37 million) for organizations.

13.4 Exceptions

In some situations, OAK Possability does not need to notify the OAIC. These are:

- Effective remedial action – if action is taken, and is reasonably considered to have been effective in minimising the risk of compromised access to information, then reporting is not necessary,
- Two or more entities – holding the same personal information and the same data breach involves more than one entity then only one entity needs to notify (If none notify, however, then both/all are in breach of the notification requirements).

Roles and Responsibilities

Title	Responsibility
Management	• Supporting, endorsing, enforcing and reviewing this policy, proceduresand any related guidelines. • Ensuring persons to whom this policy applies are educated as to the meaning and application of this policy and its procedures.
Employees	• Ensuring they understand and apply this policy, its procedures and any related guidelines.

Document Control

Reviews

The policy is to be reviewed every 3 years unless otherwise stated in audit schedule, or if the following occurs:

- An issue or improvement is identified relating to the policy and/or procedure.
- A critical incident occurs requiring a review.

References: References and documents relevant to this document are listed below.

Type	Reference
Policies	03CLI-020 Consent 03CLI-024 Complaints, Compliments and Feedback 04HUR-210 Values and Code of Conduct – Item 4 Privacy and Confidentiality 01QUA-020 Clear Desk and Clear Screen 01QUA-032 Document Management and Control
Manuals	01QUA Manual – Item 5 Confidentiality
Forms/Documents	CLI-002 Authorisation to Receive and Release Information. CLI-060 Grievance Notification and Action Report (Client) HUR-F021 Collection of Employee Information
Templates	
External References Legislation/Standards	Australian Privacy Principles (January 2014) Disability Services Act 2012 (TAS) Do not Call Register Act (2006) Freedom of Information Act 1982 National Disability Services Standards 1993 Privacy Act 1988 Privacy Amendment (February 2018) Spam Act (2003)

Version Control and Change History

Version	Effective from	Amendment
001	23/03/2018	Combination of previous Confidentiality and Privacy policies.