OstaraAustralia

RECRUITMENT. TRANSFORMING LIVES

PRIVACY & CONSENT POLICY

POLICY STATEMENT

Ostara Australia is committed to full compliance with its obligations under privacy legislation including Privacy Principles stipulated in the Privacy Act 1988 (Cth).
Ostara Australia provides all individuals with access to information regarding the privacy of their personal information.

For clients, this information is provided at their first visit and wherever possible, this information will be provided to them in the relevant language via a translation service.
Where appropriate, Ostara will also periodically remind individuals of their rights and responsibilities regarding privacy and access to information.

Ostara Australia as a Disability Employment service is required to gain and document an individual's consent prior to sharing personal information within and external to Ostara Australia and prior to the commencement of service.
All clients are assumed to have the capacity to consent unless otherwise proven. Personal information may be provided to other agencies, services, or health providers if the individual provides consent (written or verbal) that is voluntary and informed.
Personal information may also be disclosed in connection with the performance of a duty or the exercise of a power or function in accordance with relevant legislation (such as an emergency or disaster).

Employees must not, without lawful authority, destroy or damage any personal records required to be kept in accordance with the relevant legislation or regulations. Personal information will be retained and disposed of in accordance with appropriate retention and disposal guidelines referred too in this document.

Privacy Information

- Client files or information is not to be kept on the desk of any Ostara employee.
- Whiteboards or other record management signage indicating clients should have them deidentified or be unable to be seen by clients within an office
- All Ostara computers are to be locked when an employee isn't residing at their desk
- As per the departmental guidelines and the IT Ostara guidelines, passwords and logins are confidential and must not be shared with other staff or recorded.
- Staff are to use JSID as the identifier in all correspondence relating to clients
- Calls to clients are to be made privately, staff are to be mindful of other clients in offices and staff within proximity.

Evidence of Informed Consent

Consent Forms should be completed annually at minimum to ensure the client understands the consent they have allowed and to ensure they have a clear understanding of the authorised consents.

- **Ostara Permission to Disclose Forms** must be completed at an initial appointment with a jobseeker on commencement of our service and completed at minimum annually. This form allows us to understand the consents to contact a represent a client to third parties, contact allied health services and an emergency contact or carer if we are unable to reach them.
- **Audit Consent forms** are completed solely for the purpose of auditing.
- **DES Privacy consent form** is required from the client to allow staff to access their records with the department and its systems.
- **RTO consent form** is for the service to discuss training needs and supports with a registered training organisation where a client may be completing training.

PROCEDURES

The following Privacy Principles stipulated in the Privacy Act 1988 (Cth) underpin the approach used by Ostara when dealing with personal information:

- Ostara collects and holds information to provide a safe working environment, high quality service to clients and to meet obligations contained in funding and service agreements. Personal information that is collected may include an individual's name, date of birth, contact details, medical records and for client's case notes from each appointment. Personal information may be used for quality improvement and accreditation purposes.
- Personal information is only ever released if required by law or requested by an individual in relation to their own personal file. Complaints about perceived or suspected breaches of privacy will be dealt with according to Complaints Policy and Procedure. We welcome all feedback and complaints and respond as soon as possible.
- Collection of solicited personal information. Ostara will not collect personal information (other than sensitive information) unless the information is necessary for employment or service provision. Sensitive information, such as the individuals' racial or ethnic origin, sexual preferences and health information must not be collected unless the individual consents and the information is reasonably necessary.
- Dealing with unsolicited personal information. If Ostara receives information that was not solicited and is not necessary for employment, provision of the service and/or to meet funding obligations, it will be destroyed as soon as practicable or de-identified.
- Notification of the collection of personal information. Clients will be provided with information booklet – Welcome to Ostara and a privacy statement. Employees confirm the client has received and the client understood this information during their first appointment or session with the service and this is recorded in the client's file. DES Consent forms and Ostara Consent forms are mandatory compliance requirements.
- Employees are provided with access to their rights and responsibilities within the Ostara Code of Conduct in conjunction with their individual contract of employment.
- Use or disclosure of personal information in special circumstances include requests from a locating body (such as the Police) to locate a person reported as missing and disclosures to appropriate entities during emergencies and disasters. Information is only used or disclosed to provide a safe working environment, service, meet legal obligations or for quality improvement purposes. If information is to be used for a different purpose, this would normally constitute a secondary purpose and consent would be obtained using a Public Interest Certificate.
- Personal information will only be provided to a third party if consent has been given and documented in the individual's file, or if required by law. Personal information of a client may be emailed if the client is de-identified or the email is encrypted. When client data is sent via facsimile, it includes an Ostara template cover letter. The use or disclosure of information in special circumstances must be handled in consultation with the relevant General Manager or Compliance manager to ensure that appropriate criteria are considered, and that necessary documentation is kept.
- Direct Marketing. Personal information will not be disclosed for the purpose of direct marketing, that is, to promote Ostara services requires a good news story consent form to be completed by the client.
- All reasonable steps are taken to ensure that information is complete, current and accurate. Client information that is sent or received via email is included in the client file maintained in a lockable filing cabinet within an Ostara Office. We encourage the use of only digital

- Ostara takes reasonable steps to ensure that information is protected from misuse, loss and unauthorised access. Where possible, this information is kept securely in a password protected electronic database and access is determined by the security structure within the IT department. All personal information in hard copy papers are secured within the hard file. Hard copy files are always stored in a secure place and kept in locked cabinets when not in use.
- A client may request and must be offered the opportunity to have their appointment in an closed room for concerns to their privacy and confidentially. Where possible, we encourage all staff to always use private spaces where available.

Data Breach

In the event of a suspected/actual data breach the notifiable Data Breaches Act 2017 is to be followed. Notifiable Data Breaches include:

- o unauthorized access to information,
- o unauthorized disclosure of information or
- o a loss of information.

Remedial action that prevents the likelihood of serious harm will occur in the first instance.
In circumstances where Ostara Australia is unable to prevent the likelihood of serious harm or cannot prove that likely harm has not occurred, and individual(s) affected the Department are notified immediately. "Serious Harm" can be psychological, emotional, physical, reputational, or other forms of harm. Breaches to security through information technology are managed by the IT Department at Ostara and using protective programs.

File Note/ Record Content

The following guidelines must be used when completing file notes:

- Ostara should be aware that clients are entitled to make a request to view their file at any time and that appropriate processes need to be followed.
- File notes should provide a defensible position for employees and for Ostara in case of any legal action.
- Once a file note is finalized in the applicable record management system it should not be deleted from the client's record (even if it is incorrect).
- If a client requests an amendment to their progress notes, the original note may be 'revoked' and the amendment made.
- All file notes should provide a legible and accurate record of services required and services provided and any proposed action following an appointment.
- A file note should be completed for each service contact, and any attempted contacts, administration notes and supports provided.
- It is assumed that file notes will be made on the day of client contact or other recordable activity occurs. It is acceptable to record file notes up to 24 hours after client contact when it is not possible to record on the day of contact
- Progress notes should be factual. They should provide a substantiated overview of the appointment and services provided. Describe what was said or what was observed. Avoid phrases that assume what the client thinks or feels. Use statements such as … "the client appears to", "the client stated …."
- Specific discussion of a case in supervision sessions or case conference should be recorded in a file note.
- Note all correspondence regarding the client: including dates of faxes sent, letters received and sent.
- Employees are not to keep their own separate file notes. If notes are taken about a client, relevant parts must be added to the client's file and then the notes are to be securely destroyed (e.g. shredded or deleted) as soon as possible, in conjunction with relevant privacy principles and legislation.

Confidential Document Disposal

- Each site is provided with a blue secure document bin for the responsible for Confidential document destruction through SUEZ.
- Each site is responsible for developing procedures for ensuring the appropriate disposal of papers within the blue privacy disposal bins provided by SUEZ. They bins are to remain locked and collected once full.
- The destruction of ANY records must be done securely (e.g. shredding, burning or pulping) and MUST be done in accordance with agreed Ostara practices for disposal of information.

Confidential Document Retention

- Client information held by Ostara Australia is required to be retained and disposed of in accordance with the Department guidelines.
- Archived Files are stored at Support Services Centre (Ostara Head Office) in the storage facility.
- Records of the archived material is managed by the administrator officer.

Consent for minors (applicable to service users)

In general, consent for service given to a minor must be given by a person with parental responsibility for the child (for example, a parent or guardian). The consent process should include the parent or guardian confirming that they do have parental responsibility for the child and the legal right to consent on their behalf. Under current law both parents have equal rights to a child who is a minor unless the right has legally been removed from one parent.

Consent from both parents is desirable, although not legally required.

When employees are aware that the child's parents are separated and there is no Court Order in relation to the child, they may assume that the parent appearing for the appointment may provide consent for the child.
In cases where parents disagree with each other about consent or service, and both hold shared parental responsibility, then the employee is to make a professional judgment about whether to provide a service, keeping the best interests of the child as paramount.

DOCUMENT CONTROL

Version	Authorized by	Authorization Date	Sections	Amendment
1	V. Samaras	13.11.2020	All	Creation – K. Mercieca