privacy & confidentiality

To build and maintain trust with our clients, we need them to be fully confident they can give us personal information, that this information will be used appropriately, and always remain private and confidential.

At Everyday Champions, we have to collect and store information so we can provide a safe working environment for our clients, deliver high quality services and meet our legal requirements.

This involves collecting and managing personal information from clients and staff in accordance with relevant legislation and disposal guidelines.

This policy sets out how, why and what information we will collect, how we will use and (if necessary) disclose it, how we will protect people's personal information, and how we will uphold the rights of our clients and staff to access and correct their information.

Our privacy and confidentiality principles

- Everyday Champions will comply with, and exceed, its obligations under the Privacy Act 1988 (Cth) (the Privacy Act), the associated 13 Australian Privacy Principles (APPs), and Commonwealth and State legislation.
- All employees will be required to sign a 'Code of Conduct', which includes a commitment to upholding privacy and confidentiality, on commencement of employment and re-commit to the code each year during annual performance reviews.
- We will collect personal information in a lawful and fair way, and will only collect personal information which is necessary for us to perform our functions and activities, including provision of direct and indirect supports and services to clients and families.
- Personal information will only be collected by legal representatives of Everyday Champions, at a time that convenient for our clients and staff, and in a way that respects cultural differences.
- We take privacy and confidentiality seriously. If anyone breaches this policy, we will take disciplinary action.

What our clients and staff can expect from us

Our clients and staff can expect that we will privacy and confidentiality principles are in line with the 13 Australian Privacy Principles:

1. **We will ensure open and transparent management of personal information** - This means we will manage personal information in an open and transparent way, including having a clearly expressed and up to date privacy policy.
2. **We will respect people's right to anonymity and pseudonymity** - This means giving individuals the option of not identifying themselves, or of using a pseudonym - with limited exceptions.
3. **We will only collect personal information that is reasonably necessary for our work** - This means only collecting information directly related to our work. It also means we will always ask for consent before collecting personal information - unless there is a situation where we don't need to, for example, where an individual, in need of urgent medical treatment, is unable to consent to the collection of their health information because they're unconscious.
4. **We won't seek, or keep, any unsolicited personal information** - This means we will destroy or de-identify (as soon as practical) any unsolicited personal information we receive that we could not have collected under Principle 3, unless it is contained in a 'Commonwealth record' or it is unlawful or unreasonable to do so.
5. **We will always let our clients and staff know when and why we collect personal information about them** - This means we will take take reasonable steps to either notify our clients and staff of certain matters or to ensure they are aware of those matters that require us to collect information from them. If there are communication difficulties or there is concern about a person's capacity to give consent, we will seek the help of an advocate, interpreter or guardian to help with the collection of client information.
6. **We will only ever use or disclose personal information for the purpose we tell our clients and staff** - This means we will only use or disclose personal information in ways the individual would expect unless an exception applies. These exceptions include where:
    - the person has consented to using using or disclosing the information
    - the person would reasonably expect Everyday Champions to use or disclose their personal information for a different reason than they first expected, and that reason is related to the main reason we asked to collect the information in the first place
    - the information is required or authorised by or under an Australian law or a court/tribunal order

- there is a genuine reason that is consistent with the Australian Privacy Principles to use or disclose the information
- there is an acceptable health situation related to using or disclosing the information
- Everyday Champions reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

7. **We won't use personal information for direct marketing if it isn't appropriate** - This means we will only use people's personal information for direct marketing purposes if they gave us their details directly and if it's reasonable to expect Everyday Champions to use their information in this way. And we will always allow people to be able to opt out of any direct marketing.
8. **We won't make people's personal information available overseas** - This is important because it is difficult to make sure overseas entities use information from Australia in an ethical way. If this does happen somehow, we will be accountable and responsible.
9. **We will not use or disclose a government related identifier of an individual** - This means we won't use or disclose things like Medicare numbers, Centrelink Reference numbers, Driver's Licence numbers and passport numbers. The only time we will use people's government related identifiers are:
    - to disclose Working with Vulnerable People (WWVP) numbers as part of our obligations to screen our staff and protect our clients
    - to use National DIsability Insurance Scheme (NDIS) numbers to NDIS Plan Managers for the purpose of paying invoices for our services.
10. **We will make sure any personal information we collect is accurate, up to date and complete** - This means we take reasonable steps to ensure the personal information we collect is accurate, up-to-date, complete and relevant when we collect it and when we use or disclose it.
11. **We will keep all personal information safe and secure** - This means taking necessary steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. We will also meet our obligations to destroy or de-identify personal information in certain circumstances - in line with Government legislation. We will also:
    - Make sure information is protected by restricting computer access through individual logins and passwords and using access restrictions for client information systems so that employees see only the information relevant to their role.
12. **We will respect the right of our clients and staff to access their personal information** - This means we have to give our clients and staff access to their personal information when they request it. We will do this within 30 days,

unless we have a valid reason in line with government legislation, which include:

- we believe that giving people access may endanger the life, health or safety of any individual, or endanger public health or safety
- providing access would have an unreasonable impact on the privacy of other individuals
- the request is frivolous or vexatious
- the personal information is part of existing or anticipated legal proceedings between the individual and Everyday Champions.

13. **We will respect the right of our clients and staff to correct inaccurate information** - This means we will let our clients and staff change personal information that is inaccurate, out of date, incomplete, irrelevant or misleading.

Definitions

Personal information - includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

Sensitive information - Generally, sensitive information has a higher level of privacy protection than other personal information. Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information.

Express consent - You give express consent if you give it openly and obviously, either verbally or in writing. For example, when you sign your name (by hand, or by an electronic or voice signature). An organisation or agency must get your express consent before handling your sensitive information.

Implied consent - An organisation or agency doesn't need a person's express consent to handle their non-sensitive personal information; but they need to reasonably believe that they have a person's implied consent. It's not sufficient for an organisation or agency simply to tell a person of their collection, use or disclosure of their personal information. Unless they presented the person with an opt-out option they cannot assume their implied consent.