COAST+COUNTRY
community services

Policy 1.04 Privacy

Policy Statement

This policy records CCCSL's commitment to treating the information it collects in accordance with the Australian Privacy Principles in the Privacy Act 1988 (Cth) when obtaining, handling, and disclosing personal information obtained in connection with the provision of its services, including from living clients, Team Members and directors.

Procedures

1.04-1 Privacy Principles

The Privacy Act 1988 covers Australian organizations with an annual turnover of more than $3 million and details 13 Australian Privacy Principles. This policy has been developed in line with these Australian Privacy Principles:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

1.04-2 What kinds of personal (and other) information does CCCSL collect and store

The types of information that CCCSL collects depends on the nature of our engagement with various categories of individuals. CCCSL primarily collects information that is directly related, and necessary, to provide its services. Personal information includes a broad range of information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not or whether or not it is recorded in a material form. It includes:

- name;
- signature;
- address;
- phone number;

- date of birth;
- job title;
- occupation;
- employment history;
- educational qualifications;
- other contact details including email address and IP address ;
- employee records including PAYG payment summaries, pay slips, and superannuation fund details;
- Information included in identification documents such as driver's licence and tax file numbers;
- financial information such as bank account details;
- information obtained from third parties such as previous employers and referees and in the case of job applications, law enforcement agencies or professional associations;
- photographs; and
- facial recognition biometrics.

It may be necessary in some circumstances for CCCSL to collect some forms of sensitive information in order to provide specific services. Sensitive information has a higher level of privacy protection than other personal information and requires explicit permission to obtain and store. Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political organisation;
- religious beliefs or affiliations;
- philosophical belief;
- membership of a professional or trade associations or a trade union;
- sexual orientation or practices;
- criminal record,

that is also personal information; or

- health information about an individual;
- genetic information about an individual that is not otherwise health information; and
- some aspects of biometric information and templates.

In some circumstances, personal information may need to be provided about other individuals (eg dependants or other family members). If so, CCCSL relies on the person providing the information to have informed those individuals that their personal information is being provided.

1.04-3 How does CCCSL collect personal information?

It is CCCSL's usual practice to obtain personal information directly from the individual to whom it relates. Personal information is, however, also collected through a variety of different methods such as paper-based and electronic forms, face to face meetings, telephone, email and other communications, and social media websites. If the information is sensitive personal information, collection will only occur with the consent of the individual to whom it relates or is otherwise permitted under the Privacy Act 1988 (Cth).

At the time of collection, and provided that it is appropriate and reasonably possible and necessary to do so, the individual must be notified of:

- CCCSL's contact details;
- the reason this information is being collected;
- the consequences if this information is not collected; and
- information about CCCSL's privacy policy.

In some circumstances, CCCSL may be provided with personal information by third parties. In that event, CCCSL will take reasonable steps to ensure that the individual is made aware of the information so provided.

1.04-4 Where is personal information stored?

Personal information is stored in a manner that reasonably protects it from misuse, loss and unauthorised access, modification or disclosure.

Physical documents detailing personal information are stored in locked filing cabinets.

Digital personal information is stored in offsite password and two factor authentication protected data storage systems, which comply with ISO/IEC 27001, the current international standard for information security.

New documents should be scanned and saved in Trips, SharePoint or Deputy and the original documents shredded.

No personal information can be stored on a personal computer (whether being used on or off site).

Any physical documents that contain personal information are stored for 7 years, at which point they are shredded. Digital personal data is stored for a minimum of 7 years but may be stored indefinitely.

1.04-5 How CCCSL will use and disclose personal information

Personal information will only be used for the purpose for which it was provided. It will not be used for any other purpose, and will not be disclosed, unless one of the

following applies:

- informed consent is obtained from the individual, and where reasonably possible their written consent (recorded in their employee, volunteer, or client file) specifies the precise information and purpose for the disclosure;
- the individual has been told, or would reasonably expect, that such information may be used or disclosed for the other purpose, being a purpose which is related to the original purpose or, if the information is sensitive personal information, directly related to the original purpose;
- the use or disclosure is required or authorised by or under a law such as the Freedom of Information legislation;
- the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety, or to public health or safety;
- the use or disclosure is necessary in connection with suspected unlawful activity or serious misconduct; or
- the use or disclosure is otherwise permitted by law.

Access to personal information is restricted to those individuals within CCCSL who are authorised to access it.

1.04-6 How you can access your personal information, or ask for a correction

An individual has the right to access personal information held about them and to request corrections if the individual thinks that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. However, there are circumstances under the Privacy Act 1988 where CCCSL can decline access to or correction of personal information (eg where information is integrated with information about other people, or where the personal information held is an opinion about the individual and not an objective fact).

The rights of Team Members, clients and directors to access information about themselves is detailed in their Team Member/Board of Directors and Client Information Handbooks.

Any individual who wishes to access information about themselves should submit a request in writing to the CEO or Operations Manager.

1.04-7 How to lodge a complaint if you think your information has mishandled, and how your complaint will be handled

If an individual believes that their information has been mishandled, a complaint can be submitted in writing to the CEO or the CEO's nominated delegate and the complaint will be acted upon in accordance with our Complaints and Grievance Procedures (See Section 3 Service Delivery).

1.04-8 What happens if there is a data breach?

Privacy Amendment (Notifiable Data Breaches) Act 2017 requires all businesses subject to the Privacy Act with an annual turnover more than $3 million to undertake

certain investigations and to notify the Office of the Australian Information Commissioner and the affected individuals of an eligible data breach as soon as practicable after the Company suspects or is aware that there are reasonable grounds to believe that there has been an eligible data breach.

Data breaches occur in several 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 CCCSL;
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment;
- paper records stolen from insecure recycling or garbage bins;
- CCCSL mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address; and
- an individual deceiving CCCSL into improperly releasing the personal information of another person.

Dealing with a suspected Data Breach will form part of the Company Emergency & Critical Incident Action Plan.

1.04-9 Policy updates

This policy will be reviewed regularly and at least every 3 to 5 years and updated as required.

1.04-10 Data retention and deletion

All data is stored in CCCSL's intranet, Trips or CareMaster and is stored for 7 years, at which point it is removed to a non-indexed archive and retained indefinitely.

Data can be deleted after 7 years at the request of the service user