

SS 1.2 Confidentiality and privacy policy

Purpose

The purpose of this policy is to govern the responsible use and safe-keeping of confidential information held by Carpentaria.

Scope of policy

This policy applies to Carpentaria employees, volunteers and contractors who deliver services and supports on behalf of Carpentaria.

Policy statement

Carpentaria takes confidentiality and privacy of information entrusted to our organisation seriously. We abide by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APP).¹ All Carpentaria employees will receive training regarding appropriate practices and behaviours in response to privacy of data and information about individuals.

Every employee is required to use Carpentaria resources in accordance with the Information, communication and technology policy. In addition, every employee at Carpentaria has an obligation to keep confidential information safe from unauthorised access, alteration or disclosure; or loss, theft or misuse.

All Carpentaria employees with authorised access to confidential information held by Carpentaria are required to protect this information.

Employees will not:

- Seek personal benefit, or permit others to benefit, personally from any confidential information that comes to them as a result of their work
- Permit unauthorised disclosure or use of any confidential information held by Carpentaria
- Enter, add, change, or delete confidential information (unless authorised to do so)
- Release confidential information, other than what is required to perform their job-related duties
- Show or communicate the contents of any confidential information to any person, unless it is necessary to perform their job-related duties.

¹ Further information is available from: <<https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>>, accessed October 2018.

Employees are required to:

- Access confidential information for the sole purpose of performing their job-related duties
- Keep user passwords confidential and will not disclose them to anyone in or outside the organisation. Forgotten passwords and suspected compromises of passwords must be reported immediately
- Strive to keep confidential information from being viewed or heard by others (other than to whom the information is related e.g. the participant or their family member)
- Only dispose of confidential information by shredding, or via use of a secure shredding bin located on Carpentaria premises
- Ensure that confidential information, or devices that contain or provide access to confidential information, are kept secured when being removed from Carpentaria premises, or when left unattended in Carpentaria premises (including unattended desks and workstations)
- Report any observed breach of this policy. Breaching this policy may lead to dismissal and/or legal action.
-

Responsibility for implementation, compliance monitoring, measuring and continual improvement

Executives are responsible for:

- Ensuring all managers understand their responsibilities under this policy.
- Maintain a Privacy Breach Register

Managers, Coordinators and Team Leaders are responsible for:

- Ensuring all employees understand their responsibilities under this policy
- Providing support and education on the importance of confidentiality and privacy to staff
- Attend regular training and briefings on confidentiality and security.

Existing Carpentaria employees, new or returning employees or those transferring to a new role in Carpentaria, students on placement and volunteers are responsible for:

Complying with this policy and attending regular training and briefings on confidentiality and security.

Related policies and procedures

- Diversity and Anti-Discrimination Policy
- Provision of Information Policy
- Information and Records Policy
- Diversity and Inclusion Policy
- Volunteers and Contractors Policy
- Employee Supervision Policy
- Employee Learning, Training and Development Policy
- Management of Employee Performance Policy
- Information, Communication and Technology Policy
- Risk Management Policy (Organisational)

Term	Definition
Applications	All Information, Communication and Technology (ICT) software that connects to, or is accessed via, the Carpentaria network. Applications include but are not limited to internet, intranet, email, participant management systems, HR/payroll systems, incident management systems, financial systems and controlled documents systems.
Confidential Information	<p>This includes:</p> <p>Sensitive personal information (including but not limited to health and disability information) about any participant, employee or other individual that is reasonably identifiable</p> <p>Participant or donor account information</p> <p>Employment and payroll information, including salaries, tax information, withholdings, direct deposit information, employment conditions, termination, performance or disciplinary matters</p> <p>Internal investigation and internal audit information</p> <p>Legal information including information relating to litigation matters, attorney-client communications, and law enforcement or coronial investigations</p> <p>Carpentaria facilities management information, including security system information</p>



Term	Definition
	<p>Commercial and contractual information belonging to Carpentaria or any undertaking with which it deals</p> <p>Carpentaria finance information, including rates and investments</p> <p>Carpentaria operating plans, including strategic, business, and marketing plans</p> <p>Any other information held by Carpentaria that would cause reasonably foreseeable harm to an individual or undertaking (including Carpentaria) if unauthorised disclosure were to occur.</p>
Disclosure	Any release, exhibition or communication of information outside of approved access arrangements.
Information	All data, documents, records, information, reports, logs, images and audio-visuals that may be held, transmitted, stored or received in Carpentaria systems, applications, or in any media format (such as hard copy).
Sensitive Personal Information	<p>This means 'sensitive information' as defined by the Privacy Act 1988, but is summarised for this policy as follows:</p> <p>Health information (including disability information) about an individual, or</p> <p>Genetic or biometric information, or</p> <p>Information or opinion about an individual's racial or ethnic origin, political opinions or memberships, religious beliefs or affiliations, philosophical beliefs, trade association or trade union memberships, sexual orientation or practices, or criminal record.</p>
Systems	In relation to this policy, a set-up consisting of hardware, software, data and the people who use them.
Users	In relation to this policy, everyone who includes employees, contractors, volunteers, consultants and any business partners. Anyone who has access to any of Carpentaria's ICT systems, applications and networks. This

Policy reference number	SS 1.2	Version	1 October 2019
Effective date	1 October 2019	Scheduled Review Date	1 October 2021