Good Samaritan INDUSTRIES	*CONDUCT POLICY* **Privacy, Dignity and Confidentiality**	**No: CON:06** **Date:** 21/5/04 Revision No: 11 Date: 07/03/17

Purpose / Policy	GSI recognises its obligation to protect the privacy and confidentiality of service users, employees and volunteers of GSI services as required by the principles in the Privacy Act 1988. This policy is underpinned by the Australian Privacy Principles which aims to ensure that personal information is protected and the dignity of the individual is respected. The purpose of this policy is to establish standards of privacy, dignity and confidentiality in the organisation's dealings with prospective, present and past employees, volunteers and users of services. The policy will also outline the ways in which the data relating to an individual will be protected and comply with the Australian Privacy Principles. GSI believes that all employees, volunteers and consumers of service should receive the same level of privacy, dignity and confidentiality as is expected by the rest of the community and is committed to ensuring individuals' rights are respected.
National Standards Referenced	**Std 1** KPI's 1.1, 1.2, 1.4, 1.5 and 1.9; **Std 3** KPI's 3.1, 3.3 and 3.4

1.	**Information Collection**	**Resp.**
	Definitions: **Privacy and dignity-** Privacy relates to all information and practice that is personal or sensitive in nature. The act of ensuring and maintaining privacy and valued status in these matters will protect the rights and dignity of the individual. **Confidentiality -** Confidentiality refers to the restricted disclosure and dissemination of private information. All service users, employees and volunteers of GSI services will complete a confidentiality form agreeing to comply with the intent of this policy. **Data Protection -** Service users, employees, volunteers, parent and/or guardian, where applicable, must give their authority to release and/or obtain information from other sources. Only authorised personnel may gain access to service user/employee files.	

1.	**Information Collection (Continued/…)**	**Resp.**
	GSI will: Only collect personal and sensitive information that is pertinent to the recruitment and selection decision of employees and volunteers and/or is directly relevant to effective service delivery and GSI's duty of care responsibilities. • Collect information as part of a requirement of government funded services and programs. • Inform service users, employees and volunteers of the purposes of collecting information. • Obtain consent to collect information from third parties such as previous employers, referees, and significant others/family member/partner/carer/stakeholders. • Provide service users, employees and volunteers with a copy of GSI's privacy statement.	
2.	**Disclosure of Information**	
	• Disclosure of an individual's personal, sensitive, private or confidential information to a non GSI third party for any reason other than responding to a government or funding body instruction is prohibited, unless the individual is informed and provides written consent to do so using the Authority to Obtain and Release Information Form which they will need to sign and return. • Access to supported employee or other service user information is on a need to know basis. Discussions between Client Services staff and other GSI staff, with the exception of Executive Management, are to be relevant to the provision of providing support and duty of care. • Supported employees should be informed and, where appropriate, involved in discussions regarding disclosure of their information to any external source. • Personal and sensitive information will only be released to any external service without consent if required to do so by law or in a medical emergency.	
3.	**Handling of Personal Information (Data Security)**	
	• All GSI employees with access to personal records are responsible for protecting this information from misuse, loss and from unauthorised access, modification or disclosure. • Confidential information is **not** permitted to be stored on mobile devices such as thumb drives and USB drives except for payroll data which is encrypted on a USB drive and kept onsite in a fireproof safe. • Hard copies of personal or sensitive information must be stored in a locked filing cabinet. • Hard copies of personal or sensitive information should not be left in filing trays or on desks when the area is unattended. • Personal information that is stored in databases must be password protected. Passwords should not be given to any personnel that are not authorised to access the information.	

3.	**Handling of Personal Information (Data Security) (Continued/…)**	
	• Ensure that personal information about service users/employees or volunteers is only held by GSI offices as long as it is remains relevant to the delivery of effective services and the organisation's duty of care obligations and that personal information no longer needed will be destroyed or permanently de-identified after the statutory seven years has elapsed. • Except in connection with staff properly performing duties and obligations as employees, staff shall not copy or reproduce any of the confidential Information in any form or by any means. • Ensure that all journal notes in relation to service users are accurate, complete and up-to-date and entered into the relevant client management system. On termination of employment, staff must immediately deliver all Confidential Information in their possession, custody or control to the Manager Human Resources. Staff's access to IT systems and programs will also be ceased.	
4.	**Access**	
	GSI will do its utmost to ensure that the information it holds is accurate, up to date, complete and relevant. On request by a service user, employee or volunteer, GSI will let that person know, generally, what sort of personal information we hold, for what purposes, and how that information is collected, held, used and disclosed. • Service users, employees and volunteers seeking personal information held about them may request this information in writing to the Human Resources Coordinator. • The Manager will acknowledge the request in writing within 48 hours of receiving the request. • A suitable date and time will be arranged to view their file. • An authorised GSI Officer must remain in the room as personal information is viewed. • Files are to remain on site. Files are not to be removed from GSI premises except with the approval of the Chief Executive Officer and for audit purposes. • Removal of information from any file is prohibited. • An employee or client may request copies of information and this request will be submitted to the relevant Manager. • If the employee or client feels information in their personnel/personal file is recorded incorrectly, they have the right to have it corrected or a note made to state that the information is in dispute. This dispute shall be referred to the relevant Manager for review and response. • If information cannot be altered (e.g. third party forms, government or funding declarations), the Manager will discuss with the client why the information cannot be altered and attach an 'in dispute' note to relevant information. • If GSI refuses to correct the information it will in writing notify the individual who requested the correction. It will also advise the individual about the available mechanisms to complain about the refusal.	

4.	**Access (Continued/…)**	
	Denial of Request for information GSI will provide service users, employees or volunteer with access to information upon request by the individual or legal guardian, except to the extent that: • Providing that information would pose a serious and imminent threat to life or health of an individual; or • Providing access would have an unreasonable impact upon the privacy of other individuals; or • The request for access is frivolous or vexatious; or • The information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or • Providing access would be unlawful; or • Denying access is required or authorised by or under law; or • Providing access would be likely to prejudice an investigation of unlawful activity; or • The information would reveal information relating to a commercially sensitive decision making process. Where access is denied, the individual is to be provided with the relevant reason(s): • GSI will provide the individual a written notice of the reasons for the refusal. • GSI will also advise the individual about the mechanisms available to submit a complaint about the refusal.	
5.	**Breaches of Privacy**	
	Where a service user, employees or volunteer or other individual believes that their personal information has been breached or handled inappropriately by a staff member, or person acting on behalf of the organisation they may contact either: • Their Manager • The relevant Divisional Manager of the area where the breach is believed to have occurred; or • The Human Resources Divisional Manager Any feedback from an internal investigation will be collated and the outcome communicated to the complainant with relevant actions if a breach has been identified. Where a complainant believes that a satisfactory resolution to their complaint has not been achieved, the individual will be informed of their right to have the matter reviewed by an external, independent body, such as the Privacy Commissioner via the Manager Consumer Management.	Managers Divisional Managers

6.	**Complaints Handling**	
	Should a service user, employees or volunteer be unhappy with the way their personal information is being handled or believe that there is a breach of our obligations in relation to their privacy the Manager will refer the matter to their respective Divisional Manager or the CEO for resolution. If unable to be resolved, the employee or client can be directed to contact the Office of the Australian Information Commissioner on 1300 363 992.	Managers

Authorised: