

## **Privacy and Confidentiality Procedure**

### **Expected Outcome**

St George Community Transport (STGCT) Team Members and Consumers are aware of, and adhere to, procedures that support Australian Privacy Principles in the Privacy Act.

### **Training Requirements**

All Team Members

### **Procedure**

STGCT is committed to ensuring that details about Consumers and Team Members are kept confidential, and only disclosed with the persons' permission. This procedure is aligned to the Principles of the Privacy Act. The purpose of this procedure is to give information regarding the various aspects of service delivery where privacy & confidentiality is essential. Specific procedures regarding each topic are detailed in other parts of the Policy & Procedure manual. The Chief Executive Officer (CEO) will review all funding agreements to ensure that the organisation's Privacy procedures remain compliant with all funding requirements.

The following aspects of service provision are considered to require consideration of Privacy & Confidentiality:

### **Collection & Provision of Information**

- The only information held by STGCT about a Consumer will be information necessary to assess the need for a service and to provide the service/program. Information should be non-obtrusive and objective as possible, yet relevant and up-to-date.
- The only information held by STGCT regarding Team Members will be personal information required for the employment/recruitment of Team Members.
- STGCT will provide Consumers and Team Members information regarding the purpose and use of personal information including who will have access to this information.
- Consumers and Team Members will be informed of their right to withhold information or provide information anonymously, if applicable.
- Consumers and Team Members will be informed of how to make a complaint regarding the collection, storage or use of their personal information.

### **Access to and Disclosure of Information**

- The consent of the Consumer or Team Members must be obtained to utilise the Consumer's/Team Members name, photographs, videos or voice that identify an individual. Consent should be given using a Media Release and Image Consent form.
- The CEO and relevant Board members are the only people authorised to divulge information related to Team Members, where it is legally and ethically justified.
- Only Team Members with a need (i.e. those involved with the care or support of a Consumer, supervision of Team Members) will have access to personal information related to Consumers or Team Members.

- Consumers and Team Members will be made aware of their right to access their personal records by appointment and to request a copy of any document contained therein. When this is requested it will be done in the presence of the CEO. This right will also be made clear in Team Members Orientation Handbooks and Consumer Information Handbooks.
- Access to employee records is restricted to the CEO and/or Board personnel.
- In cases of emergencies the 'First Contact' or nominated person/advocate on the Consumer file will be contacted to make immediate decisions about wellbeing. Where a Duty of Care matter arises after reasonable discussions have concluded that a decision must be made 'First Contact' will provide permission.
- Consumers have the right to read any personal information kept about them by the Service. Requests from Consumers to access files should be referred to the CEO who should ensure that assistance is provided for the Consumer to access information on their file. A Team Member should be made available to explain any terminology to the Consumer.
- When a Consumer joins STGCT they are advised of the privacy and release of information procedures within the organisation including that information is kept confidential and is kept in locked filing cabinets or on a computer which only appropriate Team Members have access.
- Information that is passed on is marked 'Private and Confidential' and the computer protected with security firewalls.
- Personal information will only be emailed if the receiving agency can ensure the security of the information provided.
- The only people authorised to read a Consumers' file are the Consumer themselves, the Consumers' carer, the Consumers' advocate and the Consumers' legal guardian. Carers and Advocates must have the Consumers' permission, where this can be given.
- Access to some information may breach confidentiality of Team Members or another Consumer and this information may be withheld.
- Consent to Release Information Form is to be used when information is being released for any other purpose than referral.
- Personal information regarding a Consumer or Team Members may be disclosed if:
  - Informed consent is obtained from the person and this consent specifies the precise information and purpose for the disclosure;
  - There is a serious and imminent threat to an individual's life, health or safety;
  - There is a serious threat to public health or public safety; or
  - There is a legal obligation under the Crimes Act 1900 (NSW), the Crimes Act 1914, or the Coroners Act 1980 (NSW) to notify police about serious criminal offences, or the coroner's office regarding investigations involving the death of a person.
- Confidentiality is between the Consumer and agency (not particular Team Members). Team Members will inform the Consumers that they have to report any information that may impact upon the service provided to the office.

Steps	Action/Evidence	Who does it	When
1	Consumer indicates their wish for information to be released	Consumer	Anytime
2	Release of Information Form is completed	Consumer	Anytime
3	Information is released	CEO/Designated Representative	After consent obtained
4	Consent to release information filed in Consumers file	CEO/Designated Representative	After information released

## Storage of Personal Information

- Consumers or Team Members will be informed of the Service' responsibilities in relation to the protection of personal information through:
  - Consumer Handbooks;
  - Service Agreements; and
  - STGCTs Policies and Procedures regarding privacy and confidentiality.
- All computers containing information regarding Consumers and Team Members will be password protected.
- Any Sub Contractors which STGCT utilises will be required to provide confirmation that their policies and procedures comply with the appropriate privacy laws.
- The anonymity of Consumers and Team Members will be preserved for purposes of research, case presentations or conference papers.
- Personal information should only be copied when it is essential to do so. Consumer Files and Team Members Files will be filed separately to generalist service administration files.
- Consumer Files and Team Members files will be kept locked when not in use. Keys to Consumer Files and Team Members/Volunteer files will only be provided to personnel with authorisation to access these files.
- Files removed from the office should be placed inside a plain manila folder which does not identify the Consumers and Team Members.

## Length of time records are held and disposal

If a Consumer ceases to access the Service but may need to resume service at a later date, information relating to the Consumer will be kept for a period of 2 years before being archived. If the Consumer will definitely not be resuming services, Consumer's records will be archived at the end of the financial year. All information regarding Consumers will be shredded seven (7) years after they cease to receive services. In any other case involving personal records including the storage of child records will be in accordance with relevant legislation.

Steps	Action/Evidence	Who does it	When
1	All Information kept on computer is password protected	All Team Members	Ongoing
2	Filing Cabinets containing Consumer/Team Members files are kept locked with limited authorised access.	Authorised Team Members Only	Ongoing
3	Each Team Member will have a separate file created in hard copy and on computer	Management	At point of Employment or recruitment

## Notifying a Data Breach

An 'eligible' data breach has occurred when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur)
- This is likely to cause serious harm to any individuals to whom the information relates
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

## Data Breach response plan

The Chief Executive Officer and the Manager Consumer Engagement form the response team to deal with all matters related to a data breach.

Should a breach or a suspected breach occur, the following steps are to be taken:

- Notify the Response Team of the Service who will determine if a breach has occurred.
- Notify the individual involved as soon as possible by telephone and by letter with more information within 24 hours of the notification
- Apply remedial action to the situation to reduce the serious harm that can be caused. This could include changing a password, recovering documentation, engaging the support of information technology specialists or removing documentation.
- Engage the services of an Information Technology specialist if required.
- Notify the insurance company by email.
- Notify the Office of the Australian Information Commissioner.
- Raise an incident and record in the incident register. Allocate the responsibility for the follow up to a member of the Response Team and specify an immediate date for review.
- The CEO is to notify the Chairperson of the Board.
- The CEO will report the data breach at the next Board Meeting.
- The CEO will add the data breach to the management team meeting agenda.
- The management team will review and assess the data breach and develop an action plan to resolve the breach so that it does not occur again.
- Refer to doc\_427 Reporting Notifiable Incidents Policy and Procedure for any other reporting requirements.

## **Related Policies, Procedures and Other Documentation**

- doc\_039 Financial Management
- doc\_138 Consumer Rights and Responsibilities
- doc\_136 Consumer Fees
- doc\_035 Information Management Systems & Privacy
- doc\_427 Reporting Notifiable Incidents Policy and Procedure
- doc\_130 Privacy and Confidentiality Policy
- doc\_141 Media Release and Image Consent Form
- doc\_088 Team Member Orientation Handbook
- doc\_300 STGCT Consumer Information Handbook

## **Relevant Standards**

### **Aged Care Quality Standards**

1. Consumer Dignity and Choice
4. Service and Supports for Daily Living

### **NDIS Practice Standards**

1. Rights and responsibilities
2. Provider Governance and Operational Management