Foundations Care

Protocol: Privacy

The company is committed to managing information and communication consistent with best practice principles of privacy and security. The company will adopt practices that are consistent with the Australian Privacy Principles as set out in the Clauses of Schedule 1 of the Privacy Act 1988. Also refer to Division 2, S14 of the Privacy Act 1988. The company will also refer to the Children and Young Persons Care and Protection Act 1998. The following guiding principles shall apply:

1. The company shall only collect and store information that is relevant and necessary to the purpose for which it was intended by its collection.
2. Any information collected shall be stored in a manner that, as far as possible, is secured against tampering, unauthorised access, and inappropriate use.
3. Information shall not be retained beyond its purpose and will be securely disposed of once the purpose for which it has been collected has expired.

    a. For Aboriginal and Torres Strait Islander children and young people, all records must be kept permanently as per S14 of the Children and Young Persons (Care and Protection) Act.
    b. For Children and Young People (excluding Aboriginal and Torres Strait Islanders, all records must be retained for 7 years after the agency ceases to be responsible for the child or young person in care and then provided to FACS as per S170 of the Children and Young Persons (Care and Protection) Act.

4. The person to whom the information relates (or their legally appointed advocate/representative) shall at all times have the right to access any information stored concerning them and shall have the right to request that inaccuracies regarding factual information be corrected on the record. This will not apply to clinical or professional opinion or assessment which may be accessed but not necessarily altered.
5. A person whose information is stored by the company shall be made aware of:

    a. The company's approach to privacy;
    b. The information that is being stored;
    c. The purpose and method of storage and its management;
    d. How the information may be accessed by them and how they may seek its correction;
    e. To whom the information may be disclosed;
    f. Their rights with regards to privacy.

6. Persons whose information is stored by the company shall be given opportunity to lodge a privacy complaint which shall be managed by the company in the manner indicated in this document.

7. Any of the above shall be excepted where other legislation or legal requirements apply.

The Australian Privacy Principles

There are 13 Australian Privacy Principles (APP). The company will endeavour to meet these principles when working with and collecting information about individuals and their families.

The company may collect information from organisations and individuals for a variety of reasons. Information may be collected for event attendance, training purposes, information dissemination or project and research purposes. The company will not on-sell or disclose any information collected to another person, organisation or agency unless permission has been granted or where required or authorised by or under Australian law, or a court/ tribunal order.

Part 1: Consideration of personal information privacy	
APP 1: Open and transparent management of personal information	The company is committed to being open and transparent about why information is collected; how it is stored and who the information is given to where it is safe to do so for the client, staff and relevant others. In response, the company has committed to having a dedicated Privacy Officer to ensure the company complies with its own privacy processes and those legislated; respond to and manage privacy complaints and report to the Board of Directors in relation to privacy breaches and the effectiveness of privacy processes.
APP 2: Anonymity & pseudonymity	When providing information or making an enquiry to the company, individuals and their families have the right to remain anonymous or use a pseudonym.
Part 2: Collection of personal information	
APP 3: Collection of solicited personal information	The company will collect information through applications for service; surveys and feedback in relation to the quality of service delivery and the company's management. Information collected by the company will be securely stored in personal files and electronic databases.
APP 4: Dealing with unsolicited personal information	In the unlikely event the company receives unsolicited information then the company will destroy or de-identify the information as soon as practical and if lawful to do so.
APP 5: Notification of the collection of personal information	In the event the company receives unsolicited information about an individual, and if the information is relevant and is likely to have been collected through our processes, the company will inform the individual and explain how the information will be used as soon as practical.

Part 3: Dealing with personal information	
APP 6: Use or disclosure of personal information	Information will not be disclosed to another organisation or agency unless required or authorised by or under an Australian law, or a court/ tribunal order. Information collected by the company will be used for reporting statistics in relation to service delivery and client outcomes (information will be de-identified), disseminating information about upcoming community events and the company's programs and training opportunities. Information will not be used for other purposes unless the person has consented or the information is required to locate a missing person or for the purpose of a confidential alternative dispute resolution.
APP 7: Direct marketing	The company does not intend to use personal information collected for direct marketing purposes.
APP 8: Cross-border disclosure of personal information	The company stores information it collects from individuals in hard copy and electronic format, and as such, some information collected from individuals is stored in web-based databases. The majority of the company's information is hosted by the Australian-based company responsible for managing these services.
APP 9: Adoption, use or disclosure of government related identifiers	The company does not use, nor will it adopt government identifiers of any individual unless it becomes a legal requirement.
Part 4: Integrity of personal information	
APP 10: Quality of personal information	The company will take reasonable steps to ensure information collected and stored about an individual or another organisation is accurate, current and complete.
APP 11: Security of personal information	Information stored within the company's database, shared network system and intranet will only be available to those workers where it is relevant to undertake specific tasks. Where personal information is no longer required, the company will destroy, delete or de-identify the information unless it is required to be stored for a specified period of time.
Part 5: Access to, and correction of, personal information	
APP 12: Access to personal information	In the event the company is unable to provide access to information, it will provide the reason access was not granted and details about how to make a complaint in relation to the decision.
APP13: Correction of personal information	In the event the company is notified that information it has stored or disseminated to others is inaccurate, the requested changes will be made as soon as practicable after receiving written notification. Where the company is unable to make the requested changes, it will provide a reason for the decision and information about how to lodge a complaint in relation to the decision.