1. Scope

All staff, contractors and volunteers in relation to all individuals and their families or support networks. This document sets out the management of personal information and can be available on request or via the intranet.

Roles	Responsibilities
Staff	Ensuring privacy rights are respected and applied in their daily work. Attend and participate in training and development in the area of safeguarding privacy rights.
Managers	Monitoring and ensuring that privacy principles are implemented within their area of responsibility. Ensuring staff attend and participate in training and development in the area of safeguarding privacy rights.
Executive Management Team	Oversee of the embedding of safeguarding rights across the organisation. Approval of this policy and relevant materials including the Zest Code of Conduct.

2. Rationale

Zest Care needs to gather and use certain personal information about individuals. These can include Clients, their families, Support Workers, referrers, suppliers, employees, business contacts and other people or entities with which a business relationship exists or that which may need to be in contact.

This policy describes how personal data must be collected, handled and stored to meet the company's data protection standards and to fulfill obligation under the Privacy Act 1988, including the Amendment (Enhancing Privacy Protection) Act 2012, by complying with the Australian Privacy Principles (APPs)

3. Definitions

Australian Privacy Principles – refers to the thirteen principles outlining how organisations should collect, update, use, secure, or where necessary, disclose and give access to, personal information. This includes instructions as to how complaints should be handled and how, in some circumstances, anonymity can be maintained.

Individual – in the context of this policy means any individual person engaged in our services eg. Clients, their family members, carers or support persons and staff.

Other Party – any other person, organisation, stakeholder, entity or contact outside Zest Care.

Confidential Information - includes any documentation or information marked as confidential and any information received or developed during the course of employment, which is not publicly available, and relates to the clients or their support people with whom Zest Care interacts. This also includes the processes, and business information used by Zest Care in the course of business such as: business, financial and marketing plans and material, manuals of any kind, business projections, market or sales forecasts, pricing and product information, gross profit and cost information, business connections plans, models, methods of operation, and the nature and content of contracts and documents.

Sensitive Information – with reference to the Privacy Act 1988 means information that pertains to an individual's racial or ethnic origin, political opinions or membership of a political association, religious beliefs or affiliations, cultural heritage, philosophical beliefs, membership of a professional or trade association/union, sexual preferences, criminal history, personal health and medical information.

Personal Information – with reference to the Privacy Act 1988 refers to any information or opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not.

Permitted General Situation - as described in 16B of the Privacy Act 1988, relates to the collection, use and disclosure of personal information in cases such as serious threat to life, health, suspected unlawful activity, location of a missing person, exercise of defense.

Permitted Health Situation - as described in 16B of the Privacy Act 1988, relates to the collection, use and disclosure of personal information necessary to provide a public health service or protect public health safety.

4. Application/Strategies

Information collected and stored may include, but is not limited to, name, current and previous address, telephone number(s), driver's licence number, bank account details, Tax File Number, date of birth, diversity status, and relevant sensitive (e.g. health) information. Where reasonable and practicable to do so, we will collect personal information directly from the individual.

In some circumstances, individuals may provide some information anonymously unless:

- required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves or;
- it is impracticable for us to deal with individuals who have not identified themselves.

Personal health or business information will not be collected, updated, used, stored or disclosed to any other party without consent from the individual who the information belongs to.

Only personal information that is directly related to individuals and necessary for that purpose is collected and is done so by lawful and fair means, without unwarranted coercion.

When, or as soon as practicable after, collecting personal information from an individual, all reasonable steps are taken to ensure that they and/or their families are aware of:

1. our identity and contact details

2. how to access and update the information (Records Management Policy)
3. the purpose for which the information is collected
4. the types of entities to which we usually disclose information of that kind, and, where relevant, the countries in which overseas recipients are likely to be located
5. any law that requires the particular information to be collected
6. the main consequences (if any) for the individual if all or part of the information is not provided
7. how to complain about a breach of the Australian Privacy Principles (Complaints Policy)

When personal information about individuals is collected via a third party source, all reasonable steps are taken to ensure that the individual is made aware of the matters listed above, except to the extent that doing so would pose a serious threat to the life or health of any individual.

Individuals are informed of the necessity for collecting, using, storing or disclosing personal information and of any adverse impacts if all or part of the information is not provided.

Collection sources include:

- Direct from individuals
- From third parties and case managers in relation to case management plans and specialist requirements
- Directly from individuals applying for employment as part of the recruitment process, or training services, on an application form
- From third parties, such as previous employers or organisations for the purposes of obtaining employment reference checks or credit checks prior to the opening of an account with us

Information collected is used to provide the services as requested by individuals. This may include:

- home support services
- management of those services for consistent high-quality person-centred care
- evaluating service effectiveness and for continuous improvement planning
- responding to and resolving complaints in line with complaint management policy and procedures
- conducting appropriate police checks, “Working with Children”, and verifications and other pre-employment checks e.g. employment references
- informing participants of additional Zest Care services on offer

Staff and managers are aware of this privacy policy and provided information and training regarding the handling of personal and sensitive information. No personal information or business details can be disclosed without the prior knowledge and consent and under the guidance of the Manager.

4.1. Unsolicited information

On receipt of any unsolicited personal information, management determines whether or not the information could have been collected by lawful and fair means.

Upon determination that information could not have been collected by lawful means, and the information is not contained in a Commonwealth record, it is de-identified and destroyed, but only if it is lawful and reasonable to do so.

Upon determination that the information was collected by lawful and fair means, Australian Privacy Principles are applied to the information, as if we had collected the information under said Principles.

4.2. Disclosure

Zest Care will not disclose an individual's personal information to a person, body or agency unless:

- The individual is reasonably likely to have been aware that information of that kind is usually passed to that person, body or agency
- The individual has consented to the disclosure
- Zest Care believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual.
- the disclosure is required or authorised by or under law
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, a record of the disclosure is retained.

A person, body or agency to whom personal information is disclosed will not use or disclose the information for a purpose other than the purpose for which the information was given to the person.

4.3. Staff requirements

Staff are obliged to:

- comply with laws which require privacy and laws which require disclosure
- treat all information received in a professional manner to protect the privacy and confidentiality of families and individuals
- maintain the secrecy of Confidential Information and prevent its unauthorised disclosure to, or use by, another person
- immediately notify management of any unauthorised disclosure or use of the Confidential Information of which they become aware,
- treat all information as confidential if they are uncertain, until they are otherwise notified in writing
- maintain confidentiality, even after concluding employment with the service.

Staff may not:

- remove any Confidential Information from the Office without written authorisation
- copy, memorise, translate, extract, summarise, reproduce or reverse engineer any of the Confidential Information
- discuss clients, client's supports, client's children or children and families engaged with Department of Communities and Justice, with anyone except permanent staff employed
- reveal any information regarding the client, client supports, children, family, or family home, or Support Workers, on any social media platform (Facebook, Twitter, etc.), or by any other means (even if the information is anonymous).

4.4. Data quality and correction

All reasonable steps will be taken (as applicable) to ensure that the personal information collected, used and where appropriate, disclosed to others, is accurate, complete and up to date.

All requests for correction of personal information are actioned and confirmed, having regard to the purpose for which it is held, that the information is accurate, up to date, complete, relevant and not misleading.

On correcting personal information about an individual (that was previously disclosed to another organisation also respondent to the Australian Privacy Principles), and if an individual requests us to do so, all reasonable steps are taken to give that notification unless it is impracticable/unlawful to do so.

Individuals are provided with a written notice if we refuse to correct the personal information, as requested, setting out:

- the reasons for the refusal (except to the extent that it would be unreasonable to do so)
- the mechanisms available to complain about the refusal, and
- any other matter prescribed by the regulations.

Should a disagreement with the individual occur in relation to whether the information is inaccurate, incomplete, out of date, irrelevant or misleading, and an individual asks to associate with the information a statement that the information is inaccurate, incomplete, out of date, irrelevant or misleading, all reasonable steps are taken to associate the statement in such a way that will make the statement apparent to users of the information.

4.5. Data Security

Information held is protected from misuse, interference and loss as well as from unauthorised access, modification or disclosure.

Limited access will be given to authorised personnel only, and only where reasonable necessity for that information exists in order to provide services or in order to perform roles.

Physical, electronic, and procedural safeguards are in place that comply with federal regulations to protect personal and business information about an individual.

Information is stored securely, electronically or in paper files secured in locked cabinets. All appropriate steps are taken to destroy or permanently de-identify personal information if it is no longer required, is not contained in a Commonwealth record, and is not required by or under an Australian law, or a court/tribunal order, to be retained.

4.6. Right to access personal information

An individual has the right to access any information we hold about them, subject to some restrictions listed in Federal Government legislation. For example:

- if providing access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety
- if providing access would have an unreasonable impact upon the privacy of other individuals
- the request for access is frivolous or vexatious
- the information relates to existing or anticipated legal proceedings between an individual and us, and would not be accessible by the process of discovery in those proceedings
- providing access would reveal our intentions in relation to negotiations with an individual in such a way as to prejudice those negotiations
- providing access would be unlawful
- denying access is required or authorised by or under an Australian law or a court/tribunal order

- there is reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, is being, or may be engaged in and providing access would be likely to prejudice the taking of appropriate action in the matter
- providing access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body
- providing access would reveal evaluative information generated within Zest Care in connection with a commercially sensitive decision-making process. In this case an individual is given an explanation for the commercially sensitive decision rather than direct access to the information.

We will respond within one week of a manager receiving an access request. If any reasons for refusal apply, we will provide the reason for refusal in writing.

If access is authorised by the manager, access may be granted in a way that meets the needs of both parties, including through the use of a mutually agreed intermediary.

If an individual considers their personal information to be incorrect, incomplete, out of date or misleading, an individual can request that the information be amended. Where a record is found to be inaccurate, a correction will be made.

An individual is able to access their own records by requesting this in writing to the Manager.

5. References (legislation)

Privacy Act 1988 and amendments
Freedom of Information Act 1982
Australian Privacy Principles

6. Associated Procedures

Complaints Handling Policy and Process