1.27 PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

Purpose

ISP employs a diverse workforce of dedicated and skilled professionals committed to providing quality care to vulnerable people while upholding the values of the organisation (Community, Dignity, Justice and Integrity). This document is designed to outline the employment practices of the organisation specific to the DHHS Best Practice standards in relation to confidentiality.

Scope

This policy and procedure is applicable to all staff of ISP. It applies to the collection, storage, use, disclosure and access to consumer, carer, staff, parents/ guardians, volunteers and student's information. This procedure is aligned with the legislative requirements as set out in the *Privacy Data Protection Act 2014 (VIC)*, the *Health Records Act 2001 (VIC)* and the *Privacy Act 1988 (Cwth)* as well as the general protections for the right to privacy contained in the *Charter of Human Rights and Responsibilities Act 2006 (VIC).*

This Policy may be amended or removed at any time at the discretion of ISP.

Definitions

Confidentiality: the responsibility of holders and recipients of personal information to ensure that it is not shared in any way with unauthorised users.

Personal Information: any information or opinions that are recorded in any form (including photos and videos), whether true or not, about an individual whose identity is apparent or can reasonably be determined from that information or opinion. Personal information is any information that can be linked to an individual such as name, address, sex, age, financial details, marital status, education, criminal record or employment history, but does not include information to which the *Health Records Act 2001* applies.

Sensitive information: a type of Personal Information that is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, sexual preference or practices or criminal record.

Health Information: a type of Sensitive Information that is information or an opinion about the physical, mental or psychological health (at any time) of an individual, or a disability (at any time) of an individual. It also includes any information or opinions about health services provided to or to be provided to an individual or the individual's desires regarding future health service provision.

Confidential information: the information of a confidential nature that relates to the business of ISP and includes but is not limited to:

- Financial, budgetary, marketing, research and business plan information;
- Any information which contains trade secrets concerning ISP's business (or any of our contracting agencies) or any information relating to any other person or organisation which has been provided to ISP on a confidential basis;
- Consumer and staff information;
- Supplier and distributor lists and information;
- The terms of any contract, agreement or business arrangement with other parties;
- Information which, if published, may be detrimental to ISP's interests; and
- Licenses, intellectual property and related information.

In confidence: a request from a person other than the consumer or another health service provider that information that they have given about that consumer, not to be communicated. Information held in confidence is only to be recorded if it is relevant to the provision of service, and is to remain confidential.

***Consent*:** the agreement of a consumer, their authorised representative, or a staff member to the fulfilment of a proposed action. Consent can be expressed or implied and must be current, informed, specific and voluntary. The consumer or staff must have the *Legal Capacity* to give consent.

Informed Consent: means that a consumer or staff (or other) is provided with enough information (in appropriate forms/language that can be understood), which allows a reasonable understanding of the effects of providing consent.

Primary Purpose: the disclosure of a client's information that the client would expect is necessary to deliver the service.

Secondary Purpose: other Purposes outside the primary Purpose that ISP may have for the information such as data for service planning, reporting etc.

Information Privacy: The rights of an individual to retain some control over the way their information is collected, the way in which it may be used and who it may be disclosed to. It also relates to the rights of an individual to access information relating to their own person, to ensure that the information is correct and not misleading.

Security: is the set of procedures, techniques and technologies used to protect information from malicious or accidental destruction, alteration or access.

Policy

- ISP takes the issue of confidentiality seriously. ISP believes that all consumers, staff, contracting organisations, parents/ guardians, volunteers and students on placement

have the right for their personal information to remain confidential.

- It is the commitment of ISP that all staff act in accordance with the *Privacy Data Protection Act 2014 (VIC)*, the *Health Records Act 2001 (VIC)* and the *Privacy Act 1988 (Cwth)* as well as the general protections for the right to privacy contained in the *Charter of Human Rights and Responsibilities Act 2006 (VIC).* This means that:
    - Information will only be collected and used for the purpose for which it was collected;
    - The person whose information is being collected knows why their information is collected and how it will be used;
    - The use and disclosure of information will only occur with the person's consent except where otherwise required or authorised by law;
    - Information collected will be stored securely and will be protected from unauthorised access;
    - Any transfer of information outside of Victoria is done so subject to privacy legislation;
    - Any information collected is retained for the period authorised by the *Record Principles 2014*;
    - Any person has access to their own information and the right to ensure it is correct;
    - Information collected must be accurate and current; and
    - All staff of ISP must be made aware of their responsibilities in maintaining privacy and confidentiality.

Collection of information

- ISP may collect Personal Information in a variety of circumstances including when contact is made with the service, to enquire or use our programs either directly or via relevant government agencies and other authorities. Information may also be collected when goods or services are provided or a potential staff member applies for a job with the organisation.

- ISP may also collect personal information about interactions including any contact made without limitation to phone, email or online. For security, quality assurance, training and other purposes, we may monitor and record your communications with us (including telephone, email or online) and operate camera, video and audio surveillance devices in or outside our premises.

Use and Disclosure of personal information

- ISP staff will only use and disclose information about an individual when it is in the service of the intended Purpose (primary or secondary) of that information, and in accordance with law.

- Whenever possible, consumer information used in reports produced by ISP will be de-

identified (except if required as part of funding requirements or when necessary for a confidential report such as incident investigations).

- There may be times where ISP staff are required to collect, use or disclose consumer information as required by law. These circumstances are strictly defined and include: where the organisation believes that the disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health safety or welfare; or where the organisation believes that the disclosure is necessary to lessen or prevent a serious threat to public health, public safety or public welfare.

- In some situations, information may be used for a secondary Purpose (E.g.: A referral to an outside organisation). In some cases, this may be entities who provide services to consumers such as other community sector agencies. When information is used for a secondary Purpose, consent must be obtained, except where legislation permits.

- It is not expected that ISP will disclose personal information to an overseas entity.

Human Resource Records

- ISP keeps records in both hard copy and electronically. All staff information remains archived for 2 years after the staff has left the agency. HR records are retained for 7 years and are then destroyed as per legislative requirements.

- ISP retains the following information for the purpose of managing its human relations requirements:
  - Professional qualifications;
  - Recruitment and appointment information;
  - Payroll information;
  - Performance and professional development of staff while engaged with ISP;
  - Leave records;
  - Any correspondence between the organisation and the staff during their time of employment with ISP;
  - Any Occupational Health and safety incident reports and staff compensation claims;
  - Any records relating to disciplinary action taken during the course of the employment with ISP; and
  - Any other information as required to be kept by law, including but not limited to, the Fair Work Regulations 2009.

Job applicants

- ISP collects personal information as part of the application for employment process. The information collected is used for the Purposes of recruitment including but not limited to, assessing whether applicants are suitable for the role and the organisation, in line with the recruitment procedure.

- To verify an individual's application details and criminal history checks ISP may exchange an applicant's information with recruitment agencies, online service providers, organisations that conduct competency or psychometric tests, referees, current and previous employers, law enforcement and background checking agencies, and educational or vocational organisations.

- Once an applicant has been advised that they were unsuccessful in their application, all personal information provided as part of the application process is destroyed. ISP will, however, retain interview notes of unsuccessful applicants for a further 12 months before they are destroyed.

Rights of Access

- Consumers, staff, and volunteers have the right to seek access to their personal information and make corrections where they feel is appropriate.

- Staff who wish to access their information are required to direct their query to the relevant manager. An appropriate response will then be determined and, on access to their personal information, a written decision will be provided within 45 days of lodging the request. Should access be refused, the refusal must state on what grounds, citing the exemption applied.

- In a residential care environment where our contracting agencies maintain consumer information, all requests from consumers should be requested back to the house supervisor of that agency to follow up.

Destruction of Unnecessary Personal Information

- Any records that contain personal information will be stored for the specific time frames as required by legislation. Following this statutory time expiring, all records will be destroyed.

Security and storage of personal information

- Any information held by ISP will be protected from unauthorised access, improper use, alteration, or accidental destruction or loss by ensuring only those who are responsible for managing and maintaining the records and management have access to the information.

- ISP will take the following preventative strategies to ensure storage of personal information is secure:
    - Access control measures for file storage areas and office spaces;
    - Locked filing cabinets where paper files are located;
    - Positioning of fax machines receiving personal information so that information cannot be viewed from public areas;

- Positioning of computer terminals so that information cannot be seen or accessed by unauthorised people;
- Provision of security systems where appropriate;
- User passwords, lockable screensavers, firewall, encryption and antivirus software used on computers and networks to protect electronic information.; and
- All staff will be subject to training and support surrounding information privacy and confidentiality during induction and throughout their time with ISP.

Breaches of confidentiality and Privacy

- ISP takes breaches of confidentiality and privacy seriously. Staff who violate the Privacy and confidentiality of a consumer, staff, contracting organisation will be considered in breach of the ISP Code of Conduct and may result in disciplinary action up to and including termination of employment.

- For DHHS Funded services a privacy breach requires a Category 1 Incident report.

Privacy and complaints

- Should an individual wish to make a complaint about how ISP has handled their information, they must contact the Manager and discuss their concerns and how they believe their privacy has been breached. This complaint will then be managed as per the Complaints/Compliments and Feedback Policy.

Legislation, Standards, Policy and Related Documents

- *Privacy Act 1988 (Cwth)*
- *Freedom of Information Act 1982 (Cwth)*
- *Freedom of Information Act 1982 (Vic)*
- *Information Privacy Act 2000 (Vic)*
- *Privacy and Data Protection Act 2014 (Vic)*
- *Public Records Act 1973 (Vic)*
- *Health Records Act 2001 (Vic)*
- *Disability Act 2006 (Vic)*
- *Children, Youth and Families Act 2005 (Vic)*
- *Charter of Human Rights and Responsibilities Act 2006 (Vic)*
- *Human Services Standards (Vic) – Information Management*
- *Privacy, Data Protection and Protected Disclosures (Terms and Conditions, Service Agreement Information Kit for Funded Organisations, Victorian Department of Health and Human Services)*
- *Aged Care Act 1997 (Cwth), and relevant amendments*
- *The Records Principles 2014 (Cwth)*
- *Home Care Common Standards (Cwth) – Information Management Systems*
- *Home Care Common Standards (Cwth) – Privacy and Confidentiality*

Relevant Organisational Documents

- *Privacy and Confidentiality Policy and Procedure*
- *Records and Information Management Policy and Procedure*
- *Continuous Improvement Plan*
- *Permission Slip*
- *Declaration of Confidentiality*
- *Client Handbook*
- *Privacy Statement*
- *Privacy Audit Form*

Monitoring and Review

- This policy and procedure will be reviewed at least two-yearly by the Management Team and incorporate staff, client and other stakeholder feedback.

- The ISP *Continuous Improvement Plan* will be used to record and monitor progress of any improvements identified and where relevant feed into service planning and delivery processes.