Information Privacy

Interchange Outer East is required to meet the requirements of the Health Records Act and the Information Privacy Act in regards to the collection, storage, use and disposal of individual's information. Interchange Outer East collects information about service users, volunteers and employees. There are 10 key principles that Interchange need to observe. The principles and Interchange Outer East's practice are:

1. Collection

Principle:
Only collect information that is required for the activities conducted by Interchange Outer East and for our compliance needs (data collection).

Practice:
Family information form designed to gather information in regards to service requirements and data needs. Volunteer information includes basic contact, emergency and service specific information, appraisal information and correspondence. Employee information includes basic contact, emergency, tax declaration, bank details, contract information, appraisal information and correspondence.

2. Use and Disclosure

Principle:
Use and disclose personal information only for the purpose for which it was collected. Other purposes require the consent of the person for the use of information.

3. Consent to Share Information

All people using IOE services are required to provide signed consent for staff to access their files. This consent is provided via the registration document.

Consent to access personal information is given by:

- The parent or guardian when the person is under 18 years of age.
- By the person receiving services if the person is over 18 years of age. Where a person has complex communication or limited comprehension of the question and its implications, a family member, guardian or independent advocate can give consent.

Interchange Outer East encourages best practice, which is to continually talk to the person who owns the file (the individual the file refers to) using an accessible method to them about what information you are collecting, updating, accessing and why.

Practice:
Information collected on the Family Information Form is accessible for all services within Interchange. Additional information file notes, emails, service agreements are recorded in family file. Volunteer and Employee information is restricted to relevant staff. No disclosure of information outside of Interchange Outer East is permitted without consent unless there is a compelling legal or moral reason to do so.

4. Data Quality

Principle:
Ensure that personal information is accurate, complete and up to date.

Practice:
Care form information and medication form are updated before each service instance, or as required through discussions between staff and families. Forms are date stamped to indicate when the last update occurred. Information that is not updated in the last 12 months needs to be checked for accuracy with the family or person involved. Volunteer and Employee information is reviewed annually to ensure it is up to date.

Other practices which assist in the provision of effective services through good information include the use of tools such as Learning logs, Communication plans, Working / Not working, One Page Profiles, Important to and for, 4 questions. This information is compiled with families and people with disabilities and is effective in ensuring people receive effective and quality service.

5. Data Security and retention

Principle:
Take reasonable steps to protect personal information from misuse, loss, unauthorized access, modification or disclosure.

Practice:
Interchange Outer East collects both electronic and hard information about families, service users, volunteers and employees.
Electronic information is stored in a data center. Physical access is controlled and monitored. Hard information is stored in a file room that is locked to prevent unauthorized access.

Employees must not misuse confidential information or intellectual property, and must maintain the integrity and security of any documents or information for which they are responsible

Staff are not permitted to transfer data, client information, documents, templates or tools to private files outside the existing network and systems or send through to their private email accounts.

In the event of a data breach where a participant, family member, volunteer or employee's privacy is breeched, an incident report must be completed and forwarded to the relevant department. Please see IOE Incident Report Policy for more information.

6. Openness

Principle:
Document clearly expressed policies on management of personal information and provide policies to anyone who asks for it.

Practice:
Policy developed and available to people who ask for it.

7. Access and Correction

Principle:
Individuals have a right to seek access to their personal information and make corrections where required.

Practice:
Interchange Outer East supports the right of access by any individual to information held by Interchange about them. To access information, people need to make a request to view the information. A time and date will be negotiated where the person can examine their information. Immediate access to a family file is inappropriate as it may contain information that compromises a third party's privacy rights.

8. Identifiers

Principle:
Only assign a number to a person if it is reasonably necessary to carry out your functions efficiently.

Practice:
The only number (alphanumeric) assigned is for the Data collection requirements of relevant funding bodies.

9. Transferring information

Principle:
If the individual requests their information be transferred to another community service provider, you are required to forward that information to the service provider.

Practice:
Interchange Outer East is happy to provide information to another service provider if requested (in writing) by an individual or family.

10. Transborder data flows

Principle:
Personal information may only be provided to another agency outside Victoria if the recipient protects privacy under similar standards.

Practice:
Interchange Outer East is happy to provide information to another service provider if requested (in writing) by an individual or family.

11. Sensitive information

Principle:
The law restricts collection of sensitive information such as an individual's racial/ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.

Practice:
Interchange Outer East does collect sensitive information to ensure the safety of all participants, good practices in meeting individual needs, and sensitive matching of staff and volunteers with service users.

12. Remote working arrangements

Principle:

There are times that office-based staff work remotely. Individuals need to be mindful of the privacy of personal information and potential risks that exist outside the office environment.

Practice:

When working remotely it is essential that work is carried out in a private space i.e. home office. Conversations where personal information is discussed should not be overheard by other members of the household.

Staff access IOE's secure network via a Remote desktop client. This may be from hardware provided by IOE or staff personal devices. Staff are not permitted to transfer data, client information, documents, templates or tools to private files outside the existing network and systems or send through to their private email accounts.

Hard copies of documents containing personal information should not be made or stored outside of the IOE office environment unless it is deemed essential as part of the staff members role.

When transporting information between locations it is the responsibility of the staff member to ensure the information is secured at all times. Employees are required to report any incidents where information is misplaced or stolen immediately.