PRIVACY AND INFORMATION MANAGAEMENT POLICY & PROCEDURE

Document Created	May 2023	Version No	4
Document Owner	Company Secretary / Legal Counsel	Approval by	CEO

1. Policy Statement

Efficient and effective administrative procedures are implemented to meet clients/ staff and all other recipients/consumers (as appropriate) and regulatory requirements. Information is used responsibly to inform the decision-making process to improve care and services provided to clients/ staff and all other recipients/consumers and effective management.

An open and transparent approach to management of personal information is taken and communicated to clients/ staff and all other recipients/consumers at the first point of contact (when data is collected) in line with the Australian Privacy Principles Policy.

https://www.oaic.gov.au/privacy/australian-privacy-principles/

Spectrum is committed to respecting and maintaining privacy of personal information, through supporting a culture for managing privacy of personal information, and monitoring systems for storing of information. Staff must ensure information is as accurate as possible and must take steps to always maintain the security and confidentiality of personal information including, but not limited to electronic information, paper-based information, and oral information such as handover and the use of telephone.

The Privacy Act requires us to have guidelines around how we collect, use, and share your personal information. Spectrum makes sure that all your personal information is kept private.

2. Scope

This policy relates to the collection, storage and release of data and information about Spectrum clients, Spectrum staff and members (Board) and other parties. This policy applies to all staff, volunteers and partners of Spectrum and focuses on supporting the control clients have over personal information about themselves.

This policy covers a broad range of laws, principles, and regulations that staff and the organisation must meet to maintain the accuracy of information and privacy of clients and staff. These can be viewed at the end of this policy document. For the steps and procedures that need to be followed, access *"Information Collection, Access and Disclosure Procedures"*

3. Definitions

Personal Information:	Personal information is information or an opinion about client, volunteer or staff member and may relate to: • Ethnicity or cultural background. • Religious beliefs • Visa status • Sexual preferences or practices • Political opinions • Union / Association membership • Criminal record
Health Information:	Part of a person's personal information and is also sensitive information. This relates to a person's physical, mental, or psychological health and or disability with respect to the past, present, future. A person's expressed wishes about future health services. Health services provided or to be provided to a person; and Information collected during treatment / care provision
Authorised representative:	Is a person acting on behalf of a Spectrum client. This may include: a guardian, a solicitor, a parent if the client is a child; or person defined by law.
Breach:	A data breach happens when personal information is accessed, disclosed without authorisation, or is lost. Under the Notifiable Data Breaches scheme, you must be told if a data breach is likely to cause you serious harm
Disclosure:	Making information accessible to others outside the Spectrum and releasing the subsequent handling of the information from Spectrum control.
Data quality:	Information that is complete, accurate, reliable, and relevant to the client and Spectrum.
Security:	Protecting unauthorised use of information and steps that Spectrum take to make sure this happens.

Sensitive information:	This includes racial or ethnic origin, political opinions, or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, visa status, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.

Privacy Officers:	Spectrum appoints a small group of managers to act as Privacy Officers (as designated). Officers act as the first point of contact for staff who have questions about privacy or information.
Primary purpose:	Information Spectrum collects from clients and others to provide services to them and to make decisions about services delivered.
Secondary purpose:	Spectrum using or sharing client information that is wider than direct service delivery

4. Privacy and Information Policy

Information comes in many formats, including electronic information, paper-based information, and oral information such as handover and the use of the telephone.

Information must be centrally stored and captured so that Spectrum has a central view of clients. The Spectrum Client Management System (CMS - Cloud Care or Gold Care) is used to catalogue, capture, and record client information, details and progress notes related to clients. The (SQL) Database of choice to record all Incidents and Feedback is Spectrum Data Warehouse.

Information must not be stored or transmitted using personal devices such as mobile telephones, iPad, or personal email.

Spectrum aims to ensure the privacy of personal information and systems to look after it. Staff must ensure information is accurate and a take steps to always maintain the security and confidentiality of personal information.

Client Information

Spectrum only uses and discloses client information to provide services and for the reasons it was originally collected. We will:

- Take reasonable steps to ensure the individual is aware of why the information is being collected, who it may be disclosed to, and the main consequences if the individual does not disclose the information, and how the individual may contact Spectrum to gain access to the information collected.
- Provide processes to support our open and transparent management of personal information include providing individual's access to our Privacy Policy and our Privacy Statement.
- Ensure that the information is provided to the individual in the way that assists them to understand the information. This may include provision of the information in different formats, explanation of the information and/or translating the information.
- Ensure that when collecting or releasing client personal information that the Spectrum gain client consent to collection information using a formal process and forms and will release information only when a client agrees to releasing it.

Information is only shared with team members on a need-to-know basis.

Staff Information

Systems are in place to ensure staff's personal information is safeguarded. See also the *Safety Screening Policy /Procedure*

Staff phone numbers must not to be given to any person outside the organisation.

Spectrum has appointed Privacy Officers to ensure that this policy is implemented and adhered to. Spectrum may appoint an external Privacy Officer who may also be accessed in the first instance to resolve privacy issues.

5. Information Collection, Access, and Disclosure Procedures

Collection of Personal Information

Sensitive information must not be collected without client consent and should only include information required by Spectrum for the provision of care and services to the client.

On admission to any program, clients must be made aware of the following information by reading the Spectrum ***Consent to Collect & Release Form*** and staff answering questions about:

- the kinds of personal information required to be collected
- how personal information is collected, stored, used, and disclosed including any overseas disclosures
- how the care recipient/consumer/authorised representative may access and or seek correction of her/his personal information
- how to make a complaint about any breach of privacy and how complaints will be handled.

Staff must organise a suitable interpreter for those clients from non-English speaking background as required.

The Spectrum *Consent to Collect & Release Form* has a section record for Consent for collection, use and disclosure of personal information. The client or authorised representative is asked to sign the consent section of the Spectrum *Consent to Collect & Release Form* policy form.

A copy of the Spectrum *Consent to Collect & Release Form Policy* and signed consent form is offered to the client. This form is then filed in the client's admission notes in Cloud Care.

Wherever possible information is collected from the individual client or the carer/representative if this is not possible.

Staff must maintain privacy when collecting information.

Use & Disclosure of Personal Information

Personal Information must only be used or disclosed for the primary purpose for which it was collected; or directly related secondary purpose that would be reasonable according to the client. For example:

- sharing relevant information between team members to provide the care recipient with care and services appropriate to their needs and preferences
- sharing information on a need-to-know basis to service departments

- continuous improvement activities including documentation/clinical audits, surveys, reviews, and data analysis activities
- staff training for employees working within the organisation
- handling of complaints
- incident reporting and or legal proceedings for example, assault, professional misconduct
- providing information in an emergency to health professionals for example ambulance officers and locum doctors
- submission of funding claims
- accreditation assessments

Refer also to the *Australian Privacy Principles Policy* https://www.oaic.gov.au/privacy/australian-privacy-principles/

Staff may disclose (communicate) health information related to a client to an immediate family member as necessary to provide appropriate care unless there is an expressed wish that the client does not want information discussed with a particular person. This includes general comments to next of kin and close relatives over the telephone.

Staff must document such discussions in the progress notes. This view of continuous client/ care recipient communication should be evident within Spectrum's CMS.

There must be informed consent for use / disclosures for other purposes where reasonable expectation does not apply for example.

The Client Consent is used on admission Spectrum to use information in the following ways:

- display of images / photographs
- display of name on doors
- birthday announcements
- the Consent to Use/Disclose Information is completed for consent for articles in the local newspaper or annual report or on the organisation's website. A copy is filed in the client's file.

The client must have options explained and have the right to refuse consent for the use of personal information for a secondary purpose.

A client may request information to be available to another health service or provide authority for another health service provider to request information. This may involve a copy or summary of the information. Such requests must be referred to the Privacy Officer (Program Manager) and processed as soon as practicable.

Personal information may be disclosed/used for a secondary purpose if it is related to a law enforcement or regulatory purpose for example, subpoena, notifiable disease, compulsory reporting of elder abuse and missing care recipient. Details of such disclosures require documentation including the date, the information was used/disclosed, the enforcement body to whom it was disclosed/use and how it was used/disclosed. Refer also to Spectrum ***Client Incident Policy***.

In the case of a subpoena the whole record is copied prior to sending by Registered Mail to the address requested. Solicitors requesting copies of records must be referred to the Executive Team.

Spectrum will seek legal advice if it is unsure about how to proceed with a court order.

Accessing Information

Clients have the right to access personal / health information kept. The authorised representative must consider if able, the client would wish to access the information.

All reasonable steps must be taken to provide access.

Wherever possible access will be provided according to the form the individual requested for example.

- inspection of documents
- a copy, ensuring the deletion / omission / protection of personal information related to others
- a verbal explanation
- a written summary of the information.

Staff must direct any request to access records to the Privacy Officer (Executive General Manager or Executive Director Business Transformation). When receiving a request, the Privacy Officer will:

- verify that the person requesting access is authorised to do so
- read the relevant documents to which the request relates to identify
- any areas that may require inspection or copying to be denied
- information that could cause serious threat to life or effect the health of the person.
- whether other individuals are identified and require information protected or de-identified.
- prepare a summary or organise the preparation of a summary of the documents, if required.
- organise a meeting with a relevant health professional such as, medical practitioner to provide an explanation, if requested.
- photocopy or organise the photocopying of requested documentation.
- set up a mutually agreed time to inspect or view documents.
- arrange for a private and convenient area to inspect or have the information explained.

Accessing Staff Information

Access to staff information is carefully controlled by Spectrum and is subject to the same laws and principles as client information. Information may be required to satisfy questions about scope of practice and safety screening. For more information on accessing information contact the Manager of Human Resources.

Accessing Client Information: for people who are not clients

The *Health Records Act (Vic)* allows for an authorised representative to act for the client if she/he is incapable of acting for her/himself.

An authorised representative may be:

- enduring Power of Attorney (Financial and Personal) or State Trustee – for finances, personal & lifestyle affairs
- Medical Enduring Power of Attorney
- guardian appointed by the Victorian Civil and Administrative Tribunal (VCAT)
- person with written authority or nominated by the client
- the Australian Privacy Act allows for a responsible person for an individual to act on her/his behalf if they are unable to do so.

A responsible person may be:

- a spouse or de facto partner of the care recipient/consumer
- a child or sibling of the care recipient/consumer who is over 18 years
- a relative of the care recipient/consumer who may be traced to or through a de facto partner, child, or sibling e.g., stepchild, grandchild, niece.

Spectrum requires proof that a person requesting client information has supporting documents to satisfy the 100-pointID check adapted from the requirements of the *Financial Transaction Reports Act 1988*.

This also applies to people appointed by Spectrum to serve - on the Board of Management, to undertake work, volunteering or contracting activities.

For advice and assistance on this issue, contact Spectrum Privacy Officers.

Correcting Information

A client or authorised representative is entitled to request information to be corrected should they believe personal information is incorrect.

Requests for correction are required in writing using the *Request to Access/Correct Information form*. A request for correction of information will be managed by the Privacy Officer who will:

- verify that the person requesting correction is authorised to do so
- request supporting evidence to verify the validity of the request

Corrected information should be attached as a change that is noted in the (CMS) file whenever possible rather than deleting information from the file. Incorrect information is to be filed to ensure it is not inadvertently used by mistake, for example, in the care recipients archive file.

In rare circumstances an incorrect diagnosis for example, related to psychiatric condition can be permanently erased from the file if the individual expresses a strong concern.

The name of the person who made the correction and the correction date must be recorded on the file where the correction was made.

A record of corrections made is also recorded in the CMS (Cloud Care) indicating and detailing the request.

The organisation can refuse to correct the personal / health information if it is believed there is lack of supporting evidence. However, a statement provided by the person should be attached to state that correction was requested.

Quality of Data

All staff and volunteers must try to ensure information collected, used and or disclosed is accurate, up to date and complete.

Clients / representatives (as appropriate) / family members should be encouraged to inform staff if information changes.

Entries in client files must be actual and factual about what staff have observed and have done, not their opinion of the client.

The records must comply with legal documentation requirements including.

- client's name on each page
- date and time of each entry
- no lines left between entries
- signed by the person making the entry and her/his designation for example, Mary Smith, Personal Carer.

Whiteout or correction tape must not be used in any client record. Any errors have a line drawn through them and are initialled

Fees for Accessing Information

A fee is not charged for access to information unless there is a large amount of photocopying/printing or time required. In these cases:

- a fee of 20c per A4 page may be charged for photocopying of records.
- a minimum charge can be made where staff are required to spend substantial time locating and preparing documents.
- where a charge is made by an Intermediary these costs may be shared or waived.
- if is believed that the costs of access would pose undue hardship on the person accessing the fee can be waived.

For more information about fees and copying information, please see the Privacy Officer.

Refusing Access to Information

Spectrum can refuse of access to information if it:

- would pose a serious threat to the care recipients' life or health. If the threat was removed by providing the information in another form, this should be offered to the person.
- would impact unreasonably on another person.
- relates to information about legal proceedings between the person and the organisation.
- the information was given in confidence.
- is unlawful.
- relates to information which would prejudice a security or legal function / investigation for example, a negligence claim
- has been given and a person is being unreasonable by asking repeatedly to access the same information, in the same way.
- is considered trivial or been made jokingly.
- would leave the organisation vulnerable related to commercially sensitive decision-making information.

The client is still able to access the facts and opinions and an explanation about how the decision was made related to them.

Where a request for access has been refused the Privacy Officer (Program Manager) must provide a reason as required. The Notification of Refusal should be completed and communicated by the Privacy Officer.

An exception to providing a reason would be if the disclosure would influence a legal investigation.

Complaints

Clients or authorised representatives have the right to make a complaint where they believe there is a breach of the client's privacy. Complaints must be recorded or communicated formally via email, registered letter or ***Spectrum feedback and complaints form*** and followed up promptly as per the Spectrum Feedback and Complaints Procedures. Complaints must also be recorded in the data warehouse with an update on the outcome of the complaint.

Use of Information for Research or Study

The use of information for research or for study purposes should be congruent with Spectrum's strategy and partnership objectives. Any request to access client records for the purpose of research must be provided in writing to the CEO stating how information will be used and how ethical issues and privacy will be protected.

Proof will usually be in the form of a completed Ethics Application that has been approved by requestor's sponsoring organisation (such as a university or health service). Written consent from the CEO is required if information is to be released for this purpose.

Where information provided for research is de-identified, no privacy issue arises unless there is no direct relationship between the use and the purpose of the initial collection. In this case.

Consent where possible and feasible should be sought,

- how the use / disclosure will tangibly benefit the public health or safety should be demonstrated,
- how ethical issues will be addressed should be demonstrated, and
- how privacy will be protected should be demonstrated.

Fundraising & Direct Marketing

Spectrum does not use personal information to contact clients and families for the purpose of fundraising such as donations, bequests, or direct marketing without written consent from clients when first collecting information.

Media

The Executive handles media issues for the organisation. All media inquiries are to be directed for the attention of the Chief Executive Officer.

Personal or health information must not be disclosed unless there is informed consent or expressed consent.

Information Breaches

The following steps should be taken if there is a situation where personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

- complete an Incident Report in Data Warehouse and inform the Privacy Officer who will take immediate steps to contain the breach and coordinate the response.
- the Privacy Officer will conduct a Risk Assessment to assess what information has been affected and the risk of harm associated with the breach and if possible, the cause and extent of the breach.

- the Privacy Officer will then consider if affected individuals should be notified to reduce the risk of harm such as identity crime, physical harm, humiliation, damage to reputation. Notification should include details of the breach, the type of personal information affected, what is being done to minimise the impact and contact details for information and assistance.
- the timing of the notification and method will depend on the level of risk e.g., immediate phone call or letter in the mail.
- the Privacy Officer will also inform senior management and the need for notifying other agencies or regulatory bodies will be determined for example, the Office of the Australian Information Commissioner, the police, professional or regulatory bodies and or other organisations that maybe affected by the breach.

A comprehensive investigation will be conducted following the incident to identify and if possible, implement preventative action such as increased security measures, staff training, review and update of policies and procedures

6. Roles and Responsibilities

The manager/supervisor is responsible for:

- Ensuring teams are aware of their responsibilities in relation to maintaining client privacy and the correct collection and storage of information
- Conducting reviews of the team's performance in relation to this policy and procedure

The CEO & Executive General Manager are responsible for:

- Responding to data breaches in relation to reporting to external agencies
- Making decisions regarding the release of de-identified information for study and research purposes
- Compliance with this policy and procedure

Privacy Officer is responsible for:

- Being the first point of contact for work force enquiries about privacy, access, and storage of information
- Being aware of state and federal privacy principles

7. Training

Managers are trained on the use of this policy at management induction including relevant systems and forms.

Ongoing training and support are provided.

8. Monitoring

Spectrum keeps up to date with legislative changes and other requirements in the areas relating to this policy, updates policy, forms and informs the organisation of any such changes.

Spectrum will periodically audit compliance with this policy and procedure through self-assessment or the internal audit system.

9. Relevant Legislation & Guidance

- The Privacy and Data Protection Act 2014 (Vic)
- Health Records Act 2001 (Vic)
- Information Privacy Principles (Vic)
- The Privacy Act 1988
- Australian Privacy Principles

10. Version Control

Procedure Review/ yearly/ Quality Manager/ Approval by Board			
Review	Date approved	Approved by	Next review due
1	Sept 2019	CEO	November 2020
2	November 2022	CEO	November 2023
3	November 2022	CEO	November 2023
4	May 2023	CEO	May 2026

Document/version control			
Date	Version	Change Made	Author
Sept 2019	1.0	Created	
November 2022	2.0	Staffing titles and includes Board members	EDBT
November 2022	3.0	Privacy Act Statement	EDBT
May 2023	4.0	Updated template	Company Secretary / Legal Counsel