Spirometry Learning Australia

Privacy & Confidentiality Policy

1. Purpose and Scope

Spirometry Learning Australia (SLA) is committed to protecting the privacy and confidentiality of participants and staff in the way information is collected, stored and used.

This policy provides guidance on SLA's legal obligations and ethical expectations in relation to privacy and confidentiality.

SLA holds two types of information which are covered by this policy, personal and organisational information.

2. Definitions

- Privacy provisions of the Privacy Act 1988 govern the collection, protection and disclosure of personal information provided to SLA by clients, staff, volunteers, students and stakeholders.

- Confidentiality applies to the relationship of confidence. Confidentiality ensures that information is accessible only to those authorised to have access and is protected throughout its lifecycle. Confidential information may be marked as such or deemed confidential by its nature, e.g. it is information that is not available in the public domain.

- Consent means voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.

- Individual means any person such as a client, staff member, Board member, volunteer, student, contractor or a member of the public.

- Organisational information includes publicly available, and some confidential, information about organisations. Organisational information is not covered in the Privacy Act (1988) but some organisational information may be deemed confidential.

- Personal information means information or an opinion (including information or an opinion forming part of a database) about an individual (Office of the Federal Privacy Commissioner, 2001). It may include information such as names, addresses, bank account details and health conditions. The use of personal information is guided by the Federal Privacy Act (1988).

- The public domain in relation to confidentiality is "common knowledge," i.e. information that can be accessed by the general public.

3. Principles

SLA is committed to ensuring that information is used in an ethical and responsible manner.

SLA recognises the need to be consistent, cautious and thorough in the way that information about clients, stakeholders, staff, Board members, students and volunteers is recorded, stored and managed.

All individuals including participants and staff have legislated rights to privacy of personal information. In circumstances where the right to privacy may be overridden by other considerations (for example, child protection concerns), staff act in accordance with the relevant policy and/or legal framework.

All staff have an appropriate level of understanding about how to meet the SLA's legal and ethical obligations to ensure privacy and confidentiality.

4. Outcomes

SLA provides quality services in which information is collected, stored, used and disclosed in an appropriate manner complying with both legislative requirements and ethical obligations.

All staff understand their privacy and confidentiality responsibilities in relation to personal information and organisational information about SLA, its clients, staff and stakeholders.

This understanding is demonstrated in all work practices.

5. Functions and Delegations

Position	Delegation/Task
Business Manager	Endorse Privacy and Confidentiality Policy. Be familiar with the organisation's legislative requirements regarding privacy and the collection, storage and use of personal information. Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to SLA**,** its clients, staff and stakeholders. Comply with Privacy and Confidentiality Policy and associated procedures.
Program Manager	Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information. Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to SLA**,** its clients, staff and stakeholders.

	Ensure systems are in place across the organisation to adequately protect the privacy of personal information and confidentiality of other sensitive information. Act in accordance with organisational systems in place to protect privacy and confidentiality. Comply with Privacy and Confidentiality Policy and associated procedures.
Staff	Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to SLA**,** its clients, staff and stakeholders. Act in accordance with organisational systems in place to protect privacy and confidentiality. Comply with Privacy and Confidentiality Policy and associated procedures.

6. Risk Management

SLA ensures mechanisms are in place to demonstrate that decisions and actions relating to privacy and confidentiality comply with federal and state laws.

All staff are made aware of this policy during orientation.

All staff are provided with ongoing support and information to assist them to establish and maintain privacy and confidentiality.

7. Policy Implementation

This policy is developed in consultation with all staff and approved by the Business Manager and Program Manager. This policy is to be part of all staff orientation processes and all employees are responsible for understanding and adhering to this policy.

This policy should be referenced in relevant policies, procedures and other supporting documents to ensure that it is familiar to all staff and actively used.

This policy will be reviewed in line with SLA's quality improvement program and/or relevant legislative changes.

8. Policy Detail

The privacy of personal information is defined by legislation (Privacy Act 1988).

At all times, SLA acts in accordance with these legal requirements which are underpinned by the policy statements 8.1- 8.6 outlined below.

SLA also strives to respect the confidentiality of other sensitive information. However, in the spirit of partnership, we share information with clients and other involved individuals and organisations (subject to consent), where it would be in the best interest of the client, or other individual, to do so.

8.1 Collection of Information

Personal information collected by SLA is only for purposes which are directly related to the functions or activities of the organisation. These purposes include:

- Enquiry about programs
- Registration and enrolment into programs
- Complaint handling.

8.2 Use and Disclosure

SLA only uses personal information for the purposes for which it was given, or for purposes which are directly related to one of the functions or activities of the organisation. It may be provided to government agencies, other organisations or individuals if:

- The individual has consented
- It is required or authorised by law
- It will prevent or lessen a serious and imminent threat to somebody's life or health.

8.3 Data Quality

SLA takes steps to ensure that the personal information collected is accurate, up-to-date and complete. These steps include maintaining and updating personal information when we are advised by individuals that it has changed (and at other times as necessary), and checking that information provided about an individual by another person is correct.

8.4 Data Security

SLA takes steps to protect the personal information held against loss, unauthorised access, use, modification or disclosure and against other misuse. These steps include reasonable physical, technical and administrative security safeguards for electronic and hard copy of paper records as identified below.

Reasonable physical safeguards include:

- Locking filing cabinets and unattended storage areas
- Physically securing the areas in which the personal information is stored
- Not storing personal information in public areas
- Positioning computer terminals and fax machines so that they cannot be seen or accessed by unauthorised people or members of the public.

Reasonable technical safeguards include:

- Using passwords to restrict computer access, and requiring regular changes to passwords
- Establishing different access levels so that not all staff can view all information
- Ensuring information is transferred securely (for example, not transmitting health information via non-secure email)
- Using electronic audit trails
- Installing virus protections and firewalls.

Reasonable administrative safeguards include not only the existence of policies and procedures for guidance but also training to ensure staff are competent in this area.

8.5 Access and Correction

Individuals may request access to personal information held about them. Access will be provided unless there is a sound reason under the Privacy Act or other relevant law. Other situations in which access to information may be withheld include:

- There is a threat to the life or health of an individual
- Access to information creates and unreasonable impact on the privacy of others
- The request is clearly frivolous or vexatious or access to the information has been granted previously
- There are existing or anticipated legal dispute resolution proceedings
- Denial of access is required by legislation or law enforcement agencies.

SLA is required to respond to a request to access or amend information within 45 days of receiving the request.

Amendments may be made to personal information to ensure it is accurate, relevant, up-to-date, complete and not misleading, taking into account the purpose for which the information is collected and used. If the request to amend information does not meet these criteria, SLA may refuse the request.

If the requested changes to personal information is not made, the individual may make a statement about the requested changes which will be attached this to the record.

SLA Business Manager is responsible for responding to queries and requests for access/amendment to personal information.

8.6 Anonymity and Identifiers

Wherever it is lawful and practicable, individuals will have the option of not identifying themselves or requesting that SLA does not store any of their personal information.

As required by the Privacy Act 1988, SLA will not adopt a government assigned individual identifier number e.g. Medicare number as if it were its own identifier/client code.

8.7 Collection use and disclosure of confidential information

Other information held by SLA may be regarded as confidential, pertaining either to an individual or an organisation. The most important factor to consider when determining whether information is confidential is whether the information can be accessed by the general public.

Staff members are to refer to the Business Manager before transferring or providing information to an external source if they are unsure if the information is sensitive or confidential to SLA or its clients, staff and stakeholders.

Organisational Information

All staff agree to adhere to the SLA Code of Conduct when commencing employment.

The Code of Conduct outlines the responsibilities to the organisation related to the use of information obtained through their employment.

8.8 Breach of Privacy or Confidentiality

If staff are dissatisfied with the conduct of a colleague with regards to privacy and confidentiality of information, the matter should be raised with the Business Manager.

Staff members who are deemed to have breached privacy and confidentiality standards set out in this policy may be subject to disciplinary action.

If a participant is dissatisfied with the conduct of an SLA staff a complaint should be raised. Information on making a complaint will be made available to participants will be found on the SLA website.

Additionally, a complaint can be taken over the phone by any staff member.

9. References

Legislation

Privacy Act 1988 (Commonwealth)

Resources

Office of the Federal Privacy Commissioner (2001). *Guidelines to the National Privacy Principles*. Office of the Federal Privacy Commissioner, Sydney.

Office of the Privacy Commissioner (2006). *Privacy Policy*, Office of the Privacy Commissioner, Sydney.